(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－138670
（P2000－138670A）
(43)公開日　平成12年５月16日(2000.5.16)

(51)Int.Cl.⁷		識別記号	Ｆ Ｉ			テーマコード（参考）
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｄ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｅ	
					６４０Ｂ	
			Ｈ０４Ｌ	9/00	６７５Ｂ	

審査請求　未請求　請求項の数４　ＯＬ　（全 16 頁）

(21)出願番号　特願平10－309713

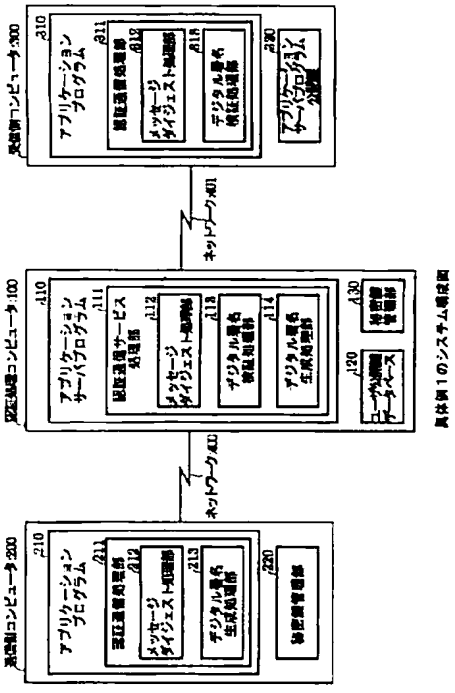
(22)出願日　平成10年10月30日(1998.10.30)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　小山　法孝
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100082050
弁理士　佐藤　幸男　（外１名）

Ｆターム(参考)　5J104 AA07 EA01 EA05 KA02 KA05
KA07 KA11 MA02 MA06 NA02
PA08 PA10

(54)【発明の名称】　認証処理方法

(57)【要約】
【課題】　デジタル署名を使用して相手認証を行う認証処理方法において、公開鍵の管理を柔軟で簡単なものとする。
【解決手段】　認証処理コンピュータ１００を単一階層構造で独立して動作するものとし、また送信者（送信側コンピュータ２００）の公開鍵を認証処理コンピュータ１００でデータベース化して管理する。



1

【特許請求の範囲】

【請求項１】　任意の通信文から取り出された固定長のメッセージダイジェストに対して自己の秘密鍵を用いてデジタル署名を生成して前記通信文に付加し通信データとしてネットワークに送信する送信側コンピュータと、公開鍵を用いて前記ネットワークからの通信データ中のデジタル署名からメッセージダイジェストを取り出し、それを同ネットワークからの通信データ中の通信文から新たに生成されたメッセージダイジェストと比較してその検証を行い得る受信側コンピュータとが前記ネットワークを介して接続された通信システムにおいて、

前記送信側コンピュータ及び受信側コンピュータ間に設けられた、単一階層構造で独立して動作する認証処理コンピュータが、前記送信側コンピュータからの通信データを受信し、自己の管理下にある公開鍵データベースに登録された送信側コンピュータの公開鍵を用いて送信側コンピュータからの通信データ中のデジタル署名からメッセージダイジェストを取り出し、それを送信側コンピュータからの通信データ中の通信文から新たに生成されたメッセージダイジェストと比較してその検証を行い、それらの一致の確認後、メッセージダイジェストから自己の秘密鍵を用いてデジタル署名を新たに生成して前記送信側コンピュータからの通信データ中の通信文に付加し通信データとして前記受信側コンピュータに送信し、この認証処理コンピュータからその公開鍵を受けて前記受信側コンピュータがその受信側コンピュータにおける前記検証を行うことで、前記送信側コンピュータ及び受信側コンピュータ間における送信側コンピュータの認証を行うことを特徴とする認証処理方法。

【請求項２】　請求項１に記載の認証処理方法において、送信側コンピュータ、受信側コンピュータ及び認証処理コンピュータは、各々分散処理環境を実装し、分散処理を行うコンピュータであることを特徴とする認証処理方法。

【請求項３】　請求項１に記載の認証処理方法において、送信側コンピュータ、受信側コンピュータ及び認証処理コンピュータは、

送信側コンピュータ及び受信側コンピュータがエージェント処理環境を、認証処理コンピュータがエージェント協調機構を、各々実装したエージェント協調システムを構成するコンピュータであることを特徴とする認証処理方法。

【請求項４】　請求項１、２又は３に記載の認証処理方法において、送受側のコンピュータ間通信は、受信側のコンピュータが複数存在するマルチキャスト通信であることを特徴とする認証処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル署名を使用して相手認証を行う認証処理方法に係り、特に、インターネットやイントラネットにおける電子メール、電子決済あるいはエージェント協調システム等での相手認証に好適な認証処理方法に関するものである。

2

【０００２】

【従来の技術】デジタル署名とは、紙ベースでの取引きにおける署名や印鑑押捺に代表される本人認証（受け手からみれば相手認証）を、通信ネットワーク等の電子メディア上で実現するためのものである。デジタル署名を使用した相手認証は次のように行われる。すなわち、通信文ｘの送信者が、送信者の秘密鍵（本人のみが知る鍵）Ｋｓを使用したデジタル署名生成アルゴリズムによって上記通信文ｘから生成したデジタル署名Ｓｉｇ（Ｋｓ，ｘ）を送信する。受信者は、送信者の公開鍵（前記秘密鍵Ｋｓと対をなし、送信者以外も知り得る鍵）Ｋｐを使用したデジタル署名検証アルゴリズムによってデジタル署名Ｓｉｇ（Ｋｓ，ｘ）を処理し、“Ｖｅｒ（Ｋｐ，Ｓｉｇ（Ｋｓ，ｘ））＝ｘ”を検証することによって相手認証を行うものである。

【０００３】デジタル署名の生成処理は、実際にはメッセージダイジェスト処理と併用されることが多い。長い文ｘからのデジタル署名Ｓｉｇ（Ｋｓ，ｘ）の生成はそれだけ時間がかかり、またコスト高になるからである。ここで、メッセージダイジェスト処理とは、任意長の元の文、上述例では通信文ｘに対して１００～１６０ビット程度、例えば１２８ビットの固定長のメッセージダイジェストＭ（ｘ）を生成する処理をいう。

【０００４】この場合、送信者は、上記のようなメッセージダイジェストＭ(ｘ)に対するデジタル署名Ｓｉｇ（Ｋｓ，Ｍ（ｘ））を上記秘密鍵Ｋｓを用いて生成し、これを上記通信文ｘと合わせて送信する。受信者は、送られてきた通信文ｘから自ら新たなメッセージダイジェストＭ（ｘ）を生成して“Ｖｅｒ（Ｋｐ，Ｓｉｇ（Ｋｓ，Ｍ（ｘ）））＝Ｍ（ｘ）”を検証する。すなわち受信者は、送信者の公開鍵Ｋｐを用いて上記デジタル署名Ｓｉｇ（Ｋｓ，Ｍ（ｘ））からメッセージダイジェストＭ(ｘ)を生成する。これを、上記デジタル署名Ｓｉｇ（Ｋｓ，Ｍ（ｘ））と合わせて送られてきた通信文ｘから、送信者が行ったと同様の手法で自ら生成した新たなメッセージダイジェストＭ（ｘ）と比較することによって、相手認証を行うものである。具体的には、上記比較結果が「一致」とでれば送信者のデジタル署名は本物であると確認（相手認証）され、また通信文の完全性（データ破壊，改ざんのないこと）が確認される。

【０００５】上述したように、受信者が送信者のデジタル署名の検証を行う時には、送信者の公開鍵を使用する必要がある。従来、多くのアプリケーションでは、受信者は、信頼できる公開鍵認証局のデジタル署名が施された公開鍵証明書を入手し、認証局のデジタル署名を検証して送信者の公開鍵を使用することになっている（ＩＴＵ－Ｘ．５０９（Ｉｎｔｅｒｎａｔｉｏｎ　Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ

Ｕｎｉｏｎ　Ｘシリーズ勧告５０９））。一方、送信者は、公開鍵証明書および後述する階層化された公開鍵認証局の各公開鍵証明書を通信文とともに送信することも可能である。この場合、受信者は、それらの公開鍵証明書が失効していないかどうかを確認するために、信頼できる公開鍵認証局から公開鍵証明書失効リストを入手する必要がある。従って、以下、受信者が公開鍵の入手を必要としているときは、送信者が公開鍵証明書を含めて送信した場合、同時に公開鍵証明書失効リストの入手を要求しているものとする。

【０００６】

【発明が解決しようとする課題】しかしながら上記従来技術には、次のような問題点があった。

（１）デジタル署名の検証で使用する公開鍵の運用，管理のためにＩＴＵ－Ｘ．５０９等で規定している公開鍵認証局は階層構造で組織化され、各認証局が協調して動作するようになっている。しかしこの構造は、階層構造の多数の認証局で公開鍵証明書のデータベースを管理する際に、その一貫性の維持、特に公開鍵証明書の取消や更新処理における各認証局の同一性の保持に困難さを抱え、しかもその迅速性の要求をも加味すると一層困難性を増し、その結果、公開鍵の運用面での柔軟性がなくなり、管理し難いという問題点があった。

【０００７】（２）デジタル署名を使用した二者間の相手認証においては、受信者が送信者毎に送信者の公開鍵を入手する必要があり、公開鍵入手処理が繁雑になり、またネットワークトラフィックが増大する等の問題点があった。

【０００８】（３）エージェント協調システムにおいて、移動型エージェント間通信を行う場合に、送信側エージェントはエージェント協調機構の協調空間にデータをプールし、他方、受信側エージェントは定期的にエージェント協調機構に問い合わせメッセージを発行して通信を実現する方式がある。このような通信方式では、各エージェントとエージェント協調機構間の通信が頻繁，複雑となり、したがって、このような通信方式に上述従来の認証処理を適用すると、処理が著しく繁雑になり、コスト高になるという問題点があった。

【０００９】（４）デジタル署名を使用した相手認証をマルチキャスト通信に適用する場合には、各受信者が、各々送信者の公開鍵を入手する必要があり、公開鍵入手処理が繁雑になり、またネットワークトラフィックが増大する等の問題点があった。

【００１０】本発明は、上記従来技術の問題点を解消すべくなされたものである。

【００１１】

【課題を解決するための手段】本発明は、上述課題を解決するため次の構成を採用する。

〈構成１〉任意の通信文から取り出された固定長のメッセージダイジェストに対して自己の秘密鍵を用いてデジタル署名を生成して上記通信文に付加し通信データとしてネットワークに送信する送信側コンピュータと、公開鍵を用いて上記ネットワークからの通信データ中のデジタル署名からメッセージダイジェストを取り出し、それを同ネットワークからの通信データ中の通信文から新たに生成されたメッセージダイジェストと比較してその検証を行い得る受信側コンピュータとが上記ネットワークを介して接続された通信システムにおいて、上記送信側コンピュータ及び受信側コンピュータ間に設けられた、単一階層構造で独立して動作する認証処理コンピュータが、上記送信側コンピュータからの通信データを受信し、自己の管理下にある公開鍵データベースに登録された送信側コンピュータの公開鍵を用いて送信側コンピュータからの通信データ中のデジタル署名からメッセージダイジェストを取り出し、それを送信側コンピュータからの通信データ中の通信文から新たに生成されたメッセージダイジェストと比較してその検証を行い、それらの一致の確認後、メッセージダイジェストから自己の秘密鍵を用いてデジタル署名を新たに生成して上記送信側コンピュータからの通信データ中の通信文に付加し通信データとして上記受信側コンピュータに送信し、この認証処理コンピュータからその公開鍵を受けて上記受信側コンピュータがその受信側コンピュータにおける上記検証を行うことで、上記送信側コンピュータ及び受信側コンピュータ間における送信側コンピュータの認証を行うことを特徴とする認証処理方法。

【００１２】〈構成２〉請求項１に記載の認証処理方法において、送信側コンピュータ、受信側コンピュータ及び認証処理コンピュータは、各々分散処理環境を実装し、分散処理を行うコンピュータであることを特徴とする認証処理方法。

【００１３】〈構成３〉請求項１に記載の認証処理方法において、送信側コンピュータ、受信側コンピュータ及び認証処理コンピュータは、送信側コンピュータ及び受信側コンピュータがエージェント処理環境を、認証処理コンピュータがエージェント協調機構を、各々実装したエージェント協調システムを構成するコンピュータであることを特徴とする認証処理方法。

【００１４】〈構成４〉請求項１、２又は３に記載の認証処理方法において、送受側のコンピュータ間通信は、受信側のコンピュータが複数存在するマルチキャスト通信であることを特徴とする認証処理方法。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態につき図面を用いて説明する。

《具体例》

〈具体例１の構成〉図１は、本発明による認証処理方法の具体例１が適用された通信システムを示すブロック図である。ここでは、認証処理コンピュータとして機能するサーバコンピュータ（以下、認証処理コンピュータと

いう。）１００が、送信側コンピュータ２００とはネットワーク４００によって、受信側コンピュータ３００とはネットワーク４０１によって、各々接続されたシステムの全体構成を示している。

【００１６】上記認証処理コンピュータ１００は、単一階層構造で独立して動作するもので、アプリケーションサーバプログラム１１０、ユーザ公開鍵データベース１２０及び秘密鍵管理部１３０を備えてなる。ここで、アプリケーションサーバプログラム１１０は、メッセージダイジェスト処理部１１２、デジタル署名検証処理部１１３、デジタル署名生成処理部１１４等からなる認証通信サービス処理部１１１を備える。ユーザ公開鍵データベース１２０はユーザ（送信側コンピュータ２００）の公開鍵を登録したデータベースで、アプリケーションサーバプログラム１１０の管理下にあってユーザのデジタル署名を検証する際に使用されるものである。秘密鍵管理部１３０は認証処理コンピュータ１００においてデジタル署名を生成する際に使用するアプリケーションサーバプログラム１１０の秘密鍵を管理するものである。

【００１７】送信側コンピュータ２００は、アプリケーションプログラム２１０及び秘密鍵管理部２２０を備えてなる。ここで、アプリケーションプログラム２１０は、メッセージダイジェスト処理部２１２及びデジタル署名生成処理部２１３等からなる認証通信処理部２１１を備える。秘密鍵管理部２２０は、送信側コンピュータ２００のデジタル署名を生成する際に使用する送信側コンピュータ２００の秘密鍵を管理するものである。

【００１８】受信側コンピュータ３００は、アプリケーションプログラム３１０及びアプリケーションサーバプログラム公開鍵３２０を備えてなる。ここで、アプリケーションプログラム３１０は、メッセージダイジェスト処理部３１２及びデジタル署名検証処理部３１３等からなる認証通信処理部３１１を備える。アプリケーションサーバプログラム公開鍵３２０は、デジタル署名を検証する際に使用されるものである。

【００１９】〈具体例１の動作〉次に、上述具体例１の動作について説明する。図２は、送信側コンピュータ２００におけるアプリケーションプログラム２１０の動作を示すフローチャートである。この図に示すように、アプリケーションプログラム２１０は、まず通信文の本体を作成し、それに予め決められた形式で送信者情報、受信者情報を付加する（ステップＳ２１）。以下、通信文本体にそれらの情報を付加したものを通信文という。

【００２０】次に、アプリケーションプログラム２１０は、メッセージダイジェスト処理部２１２を使用して通信文のメッセージダイジェストを生成し（ステップＳ２２）、続いて、秘密鍵管理部２２０で管理している送信側コンピュータ２００の秘密鍵及びデジタル署名生成処理部２１３を使用して上記メッセージダイジェストに対するデジタル署名を生成する（ステップＳ２３）。その後、上記通信文とデジタル署名を合わせてなる通信データを認証処理コンピュータ１００（アプリケーションサーバプログラム１１０）に送信し（ステップＳ２４）、送信側コンピュータ２００における通信文送信手順を終了する。

【００２１】図３に上記アプリケーションサーバプログラム１１０に送信されるデータ（通信データ）のフォーマットの概略を示す。ここでは、送信者はＡ、受信者はＢで表現されており、Ａ，Ｂは、各アドレス情報を含む。図示するように、通信文は送信者情報Ａ及び受信者情報Ｂと通信文本体とからなり、この通信文と、通信文のメッセージダイジェストのデジタル署名（メッセージダイジェストを含む。本明細書において同様。）とで通信データが構成される。具体例１では、送信者情報Ａは送信側コンピュータ２００、受信者情報Ｂは受信側コンピュータ３００となる。

【００２２】図４は、認証処理コンピュータ１００におけるアプリケーションサーバプログラム１１０の動作を示すフローチャートである。この図に示すように、アプリケーションサーバプログラム１１０（認証処理コンピュータ１００）は、まず送信側コンピュータ２００からの通信文とデジタル署名を合わせてなる通信データ（図３参照）を受信する（ステップＳ４１）。

【００２３】次に、アプリケーションサーバプログラム１１０は、デジタル署名検証処理部１１３によって送信側コンピュータ２００のデジタル署名の検証を行う（ステップＳ４２）。このデジタル署名の検証は、デジタル署名検証処理部１１３によって、以下の手順で行う。初めに、アプリケーションサーバプログラム１１０は、ユーザ公開鍵データベース１２０に登録されている送信側コンピュータ２００（ユーザ）の公開鍵を使用して、送信側コンピュータ２００のデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェスト処理部１１２によって、アプリケーションプログラム２１０からの通信文のメッセージダイジェストを新たに生成する。そして、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終了する。不一致であれば送信側コンピュータ２００にエラーを通知する。

【００２４】デジタル署名の検証後、アプリケーションサーバプログラム１１０は、デジタル署名生成処理部１１４を起動し、秘密鍵管理部１３０で管理する自プログラムの秘密鍵を使用して、上記通信文のメッセージダイジェストのデジタル署名を新たに生成する（ステップＳ４３）。その後、アプリケーションサーバプログラム１１０は、上記通信文とステップ４３で新たに生成したデジタル署名を合わせてなる通信データを受信側コンピュータ３００に送信する（ステップＳ４４）。受信者情報は、上記通信文を参照することによって知り得る。

【００２５】図５は、受信側コンピュータ３００におけるアプリケーションプログラム３１０の動作を示すフローチャートである。まず、受信側コンピュータ３００上のアプリケーションプログラム３１０は、認証処理コンピュータ１００（アプリケーションサーバプログラム１１０）からの通信文と新たなデジタル署名（アプリケーションサーバプログラム１１０によるデジタル署名）を合わせてなる通信データを受信する（ステップＳ５１）。

【００２６】次に、アプリケーションプログラム３１０は、認証処理コンピュータ１００からの新たなデジタル署名の検証を行う（ステップＳ５２）。このデジタル署名の検証は、デジタル署名検証処理部３１３によって、以下の手順で行う。初めに、アプリケーションプログラム３１０は、アプリケーションサーバプログラム公開鍵３２０を使用して、アプリケーションサーバプログラム１１０からのデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェスト処理部３１２によって、アプリケーションサーバプログラム１１０からの通信文のメッセージダイジェストを新たに生成する。そして、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終了する。検証が正常終了すると、送信側コンピュータ２００から受信側コンピュータ３００への認証通信処理が終了する。

【００２７】〈具体例１の効果〉

（１）従来技術のように各々が協調して動作する階層構造で組織化された多数の公開鍵認証局ではなく、単一階層構造で独立して動作する認証処理コンピュータ１００が送信側コンピュータ２００の公開鍵を管理するので、送信側コンピュータ２００の公開鍵の運用面で、柔軟で管理しやすいシステムを構築することができる。

【００２８】（２）従来、デジタル署名を使用した二者間の相手認証においては、受信側コンピュータが送信側コンピュータ毎に送信側コンピュータの公開鍵を入手する必要があった。具体例１では、上記認証処理コンピュータ１００がユーザ（送信側コンピュータ２００）の公開鍵をまとめて管理するので、受信側コンピュータ３００が送信側コンピュータ２００の公開鍵を個々に入手する繁雑さが省け、ネットワークトラフィック、特に送受信側コンピュータ２００，３００間にわたってのネットワークトラフィックを減少させることができる。

【００２９】〈具体例２の構成〉図６は、本発明による認証処理方法の具体例２が適用された通信システムを示すブロック図である。ここでは、分散処理環境１５０，２４０，３４０を実装する３つのコンピュータ１００，２００，３００が、コンピュータ２００とコンピュータ１００とはネットワーク４００によって、コンピュータ１００とコンピュータ３００とはネットワーク４０１によって、各々接続され、これら３つのコンピュータ１００，２００，コンピュータ３００にまたがって分散アプリケーションプログラム５００が動作するシステムの全体構成を示している。以下、３つのコンピュータ１００，２００，３００を、本具体例２における各々の機能に基づき、１００なるコンピュータを認証処理コンピュータ、２００なるコンピュータを送信側コンピュータ、３００なる受信側コンピュータという。

【００３０】上記認証処理コンピュータ１００は、単一階層構造で独立して動作するもので、上記分散処理環境１５０の他、上記分散アプリケーションプログラム５００で動作される認証パイプオブジェクト１４０、メッセージダイジェストオブジェクト１４１及びデジタル署名オブジェクト１４２と、認証パイプオブジェクト１４０の秘密鍵を管理する秘密鍵管理部１３０と、図示システム内の全てのオブジェクト（ユーザ）の公開鍵が登録されたオブジェクト公開鍵データベース１６０とを備える。このオブジェクト公開鍵データベース１６０は、認証パイプオブジェクト１４０の管理下にあってユーザのデジタル署名を検証する際に使用されるものである。

【００３１】送信側コンピュータ２００は、上記分散処理環境２４０の他、上記分散アプリケーションプログラム５００で動作されるオブジェクトＡ２３０、メッセージダイジェストオブジェクト２３１及びデジタル署名オブジェクト２３２と、オブジェクトＡ２３０の秘密鍵を管理する秘密鍵管理部２２０とを備える。

【００３２】受信側コンピュータ３００は、上記分散処理環境３４０の他、上記分散アプリケーションプログラム５００で動作されるオブジェクトＢ３３０、メッセージダイジェストオブジェクト３３１及びデジタル署名オブジェクト３３２と、認証パイプオブジェクト公開鍵３５０とを備える。

【００３３】なお、上記認証パイプオブジェクト１４０、オブジェクトＡ２３０及びオブジェクトＢ３３０は、通信手段をもち相互に通信可能である。また、メッセージダイジェストオブジェクト１４１，２３１，３３１は、各々メッセージダイジェスト生成メソッドをもち、デジタル署名オブジェクト１４２，２３２，３３２は、各々署名検証メソッド及び署名生成メソッドをもつものとする。

【００３４】〈具体例２の動作〉次に、上述具体例２の動作について説明する。図７は、送信側コンピュータ２００におけるオブジェクトＡ２３０の動作を示すフローチャートである。この図に示すように、オブジェクトＡ２３０は、まず通信文の本体を作成し、それに予め決められた形式で送信側コンピュータ２００（オブジェクトＡ２３０）情報、受信側コンピュータ３００（オブジェクトＢ３３０）情報を付加する（ステップＳ７１）。以下、通信文本体にそれらの情報を付加したものを通信文という。

【００３５】次に、オブジェクトＡ２３０は、メッセージダイジェストオブジェクト２３１のメッセージダイジェスト生成メソッドを使用して通信文のメッセージダイジェストを生成し（ステップＳ７２）、続いて、秘密鍵管理部２２０で管理しているオブジェクトＡ２３０の秘密鍵及びデジタル署名オブジェクト２３２の署名生成メソッドを使用して上記メッセージダイジェストに対するデジタル署名を生成する（ステップＳ７３）。その後、上記通信文とデジタル署名を合わせてなる通信データを認証処理コンピュータ１００上の認証パイプオブジェクト１４０に送信し（ステップＳ７４）、オブジェクトＡ２３０の通信文送信手順を終了する。通信データのフォーマットは、送信者がオブジェクトＡ２３０、受信者がオブジェクトＢ３３０になることを除いて図３と同様である。

【００３６】図８は、認証処理コンピュータ１００における認証パイプオブジェクト１４０の動作を示すフローチャートである。この図に示すように、認証パイプオブジェクト１４０は、まず送信側コンピュータ２００（オブジェクトＡ２３０）からの通信文とオブジェクトＡ２３０のデジタル署名を合わせてなる通信データを受信する（ステップＳ８１）。

【００３７】次に、認証パイプオブジェクト１４０は、オブジェクトＡ２３０のデジタル署名の検証を行う（ステップＳ８２）。このデジタル署名の検証は、以下の手順で行う。初めに、認証パイプオブジェクト１４０は、オブジェクト公開鍵データベース１６０に登録されているオブジェクトＡ２３０の公開鍵を使用して、オブジェクトＡ２３０のデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェストオブジェクト１４１のメッセージダイジェスト生成メソッドを使用して、上記通信文のメッセージダイジェストを新たに生成する。そして、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終了する。不一致であれば送信側コンピュータ２００にエラーを通知する。

【００３８】デジタル署名の検証後、認証パイプオブジェクト１４０は、デジタル署名オブジェクト１４２の署名生成メソッドにより、秘密鍵管理部１３０で管理する自オブジェクトの秘密鍵を使用して、上記通信文のメッセージダイジェストのデジタル署名を新たに生成する（ステップＳ８３）。その後、認証パイプオブジェクト１４０は、上記通信文と新たに生成したデジタル署名を合わせてなる通信データをオブジェクトＢ３３０に送信する（ステップＳ８４）。受信者情報は、上記通信文を参照することによって知り得る。

【００３９】図９は、受信側コンピュータ３００におけるオブジェクトＢ３３０の動作を示すフローチャートである。まず、受信側コンピュータ３００上のオブジェクトＢ３３０は、認証処理コンピュータ１００（認証パイプオブジェクト１４０）からの通信文と新たなデジタル署名（認証パイプオブジェクト１４０によるデジタル署名）を合わせてなる通信データを受信する（ステップＳ９１）。

【００４０】次に、オブジェクトＢ３３０は、認証処理コンピュータ１００からの新たなデジタル署名の検証を行う（ステップＳ９２）。このデジタル署名の検証は、以下の手順で行う。初めに、オブジェクトＢ３３０は、認証パイプオブジェクト公開鍵３５０を使用して、認証パイプオブジェクト１４０のデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェストオブジェクト３３１のメッセージダイジェスト生成メソッドを使用して、上記通信文のメッセージダイジェストを新たに生成する。そして、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終了する。検証が正常終了すると、オブジェクトＡ２３０からオブジェクトＢ３３０への認証通信処理が終了する。

【００４１】〈具体例２の効果〉

（１）分散処理システムにおいても、従来技術のように各々が協調して動作する階層構造で組織化された多数の公開鍵認証局ではなく、単一階層構造で独立して動作する認証処理コンピュータ１００が送信側コンピュータ２００の公開鍵を管理するので、送信側コンピュータ２００の公開鍵の運用面で、柔軟で管理しやすいシステムを構築することができる。

【００４２】（２）従来、分散処理を行うシステムでのデジタル署名を使用した二者間の相手認証においては、受信側コンピュータ（オブジェクト）が送信側コンピュータ（オブジェクト）毎に送信側コンピュータの公開鍵を入手する必要があった。具体例２では、相互に通信を行うオブジェクトＡ２３０，オブジェクトＢ３３０を備えた送信側コンピュータ２００，受信側コンピュータ３００間の認証処理コンピュータ１００がユーザ（送信側コンピュータ２００）の公開鍵をまとめて管理するので、受信側コンピュータ３００が送信側コンピュータ２００の公開鍵を個々に入手する繁雑さが省け、ネットワークトラフィック、特に送受信側コンピュータ２００，３００間にわたってのネットワークトラフィックを減少させることができる。

【００４３】〈具体例３の構成〉図１０は、本発明による認証処理方法の具体例３が適用された通信システムを示すブロック図である。ここでは、エージェント処理環境２５０，３６０，６１０，６１１，６１２，６１３を実装する複数のコンピュータ２００，３００，６００，６０１，６０２，６０３及びエージェント協調機構１７０を実装するコンピュータ１００が、ネットワーク４００，４０１，４０２，４０３によって接続されたエージ

ェント協調システムの全体構成を示している。以下、コンピュータ１００，２００，３００を、本具体例３における各々の機能に基づき、１００なるコンピュータを認証処理コンピュータ、２００なるコンピュータを送信側コンピュータ、３００なる受信側コンピュータという。

【００４４】上記認証処理コンピュータ１００は単一階層構造で独立して動作するもので、エージェント協調機構１７０を備える。このエージェント協調機構１７０は、メッセージダイジェスト処理部１７１、デジタル署名検証処理部１７２、デジタル署名生成処理部１７３、エージェント公開鍵データベース１７４、秘密鍵管理部１７５及びメッセージ記憶領域１７６を備えてなる。上記エージェント公開鍵データベース１７４には、図示システム内の全てのエージェント（ユーザ）の公開鍵が登録されている。このエージェント公開鍵データベース１７４は、エージェント協調機構１７０の管理下にあってユーザのデジタル署名を検証する際に使用されるものである。秘密鍵管理部１７５は、エージェント協調機構１７０の秘密鍵を管理するものである。メッセージ記憶領域１７６は、送信側エージェントから受信側エージェントへの通信文及びデジタル署名等を一時記憶するものである。

【００４５】送信側コンピュータ２００は、上記エージェント処理環境２５０の他、エージェントＡ２６０を備える。ここで、エージェントＡ２６０は、メッセージダイジェスト処理部２６１、デジタル署名生成処理部２６２及び秘密鍵管理部２６３を備えてなる。秘密鍵管理部２６３は、エージェントＡ２６０の秘密鍵を管理するものである。

【００４６】受信側コンピュータ３００は、上記エージェント処理環境３６０の他、エージェントＢ３７０を備える。ここで、エージェントＢ３７０は、メッセージダイジェスト処理部３７１、デジタル署名検証処理部３７２及びエージェント協調機構公開鍵３７３を備えてなる。

【００４７】図示システムのエージェントは、エージェント処理環境を実装している複数のコンピュータ間を移動する能力をもつ移動型エージェント又は１つのコンピュータ上に常駐する常駐型エージェントのどちらであってもよい。また、図示システムの各エージェントは、通信手段をもち相互に通信可能である。２つのエージェントが移動型エージェントである場合、それらは次のようにして通信可能になされている。ここでは、通信を行う可能性のある移動型エージェントは、定期的にエージェント協調機構１７０に問い合わせメッセージを発信することとする。送信側エージェントは、送信データをエージェント協調機構１７０にポストし、受信側エージェントは、エージェント協調機構１７０に問い合わせメッセージを発信した際に、自エージェント宛の送信データの存在を知り、それを得ることができるようになされている。図示システムのエージェントＡ２６０及びエージェントＢ３７０は、上述したように移動型であっても常駐型であってもよいが、どちらも移動型である場合には、上記のような通信方法で通信可能になされているものとする。

【００４８】〈具体例３の動作〉次に、上述具体例３の動作について説明する。図１１は、送信側コンピュータ２００におけるエージェントＡ２６０の動作を示すフローチャートである。この図に示すように、エージェントＡ２６０は、まず通信文の本体を作成し、それに予め決められた形式で送信側コンピュータ２００（エージェントＡ２６０）情報、受信側コンピュータ３００（エージェントＢ３７０）情報を付加する（ステップＳ１１１）。以下、通信文本体にそれらの情報を付加したものを通信文という。

【００４９】次に、エージェントＡ２６０は、メッセージダイジェスト処理部２６１を使用して通信文のメッセージダイジェストを生成し（ステップＳ１１２）、続いて、秘密鍵管理部２６３で管理しているエージェントＡ２６０の秘密鍵及びデジタル署名生成処理部２６２を使用して上記メッセージダイジェストに対するデジタル署名を生成する（ステップＳ１１３）。その後、上記通信文とデジタル署名を合わせてなる通信データを認証処理コンピュータ１００上のエージェント協調機構１７０に送信し（ステップＳ１１４）、エージェントＡ２６０の通信文送信手順を終了する。通信データのフォーマットは、送信者情報がエージェントＡ２６０、受信者情報がエージェントＢ３７０になることを除いて図３と同様である。

【００５０】図１２は、認証処理コンピュータ１００におけるエージェント協調機構１７０の動作を示すフローチャートである。この図に示すように、エージェント協調機構１７０は、まず送信側コンピュータ２００上のエージェントＡ２６０からの通信文とエージェントＡ２６０のデジタル署名を合わせてなる通信データを受信する（ステップＳ１２１）。

【００５１】次に、エージェント協調機構１７０は、メッセージダイジェスト処理部１７１及びデジタル署名検証処理部１７２によってエージェントＡ２６０のデジタル署名の検証を行う（ステップＳ１２２）。このデジタル署名の検証は、以下の手順で行う。初めに、エージェント協調機構１７０は、エージェント公開鍵データベース１７４に登録されているエージェントＡ２６０の公開鍵を使用して、エージェントＡ２６０のデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェスト処理部１７１によって、上記通信文のメッセージダイジェストを新たに生成する。そして、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終

了する。不一致であればエラーログを残しておき、次にエージェントＡ２６０から問い合わせメッセージを受信した時にそのエージェントＡ２６０にエラーを通知する。

【００５２】デジタル署名の検証後、エージェント協調機構１７０は、デジタル署名生成処理部１７３を起動し、秘密鍵管理部１７５で管理するエージェント協調機構１７０の秘密鍵を使用して、上記通信文のメッセージダイジェストのデジタル署名を新たに生成する（ステップＳ１２３）。上記通信文及び新たに生成したデジタル署名は、エージェント協調機構１７０内のメッセージ記憶領域１７６に保持しておく。

【００５３】図１３は、受信側コンピュータ３００におけるエージェントＢ３７０の動作を示すフローチャートである。まず、受信側コンピュータ３００上のエージェントＢ３７０は、エージェント協調機構１７０に問い合わせメッセージを発信する（ステップ１３１）。これに対し、エージェント協調機構１７０は、既にエージェントＡ２６０から受信していた通信文と新たに生成したデジタル署名（エージェント協調機構１７０によるデジタル署名）を合わせてなる通信データをメッセージ記憶領域１７６から読み出し、エージェントＢ３７０に渡す（エージェントＢ３７０は読み出された通信データを受け取る）（ステップ１３２）。

【００５４】次に、エージェントＢ３７０は、エージェント協調機構１７０からの新たなデジタル署名の検証を行う（ステップＳ１３３）。このデジタル署名の検証は、デジタル署名検証処理部３７２によって、以下の手順で行う。初めに、エージェントＢ３７０は、エージェント協調機構公開鍵３７３を使用して、エージェント協調機構１７０からのデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェスト処理部３７１によって、エージェント協調機構１７０からの通信文のメッセージダイジェストを新たに生成する。そして、デジタル署名検証処理部３７２によって、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終了する。検証が正常終了すると、エージェントＡ２６０からエージェントＢ３７０への認証通信処理が終了する。

【００５５】〈具体例３の効果〉

（１）エージェント協調システムにおいても、従来技術のように各々が協調して動作する階層構造で組織化された多数の公開鍵認証局ではなく、単一階層構造で独立して動作する認証処理コンピュータ１００が送信側コンピュータ２００の公開鍵を管理するので、送信側コンピュータ２００の公開鍵の運用面で、柔軟で管理しやすいシステムを構築することができる。

【００５６】（２）従来、エージェント協調システムでのデジタル署名を使用した二者間の相手認証においては、受信側コンピュータ（エージェント）が送信側コンピュータ（エージェント）毎に送信側コンピュータの公開鍵を入手する必要があった。具体例３では、相互に通信を行うエージェントＡ２６０，エージェントＢ３７０を備えた送信側コンピュータ２００，受信側コンピュータ３００間の認証処理コンピュータ１００がユーザ（送信側コンピュータ２００）の公開鍵をまとめて管理するので、受信側コンピュータ３００が送信側コンピュータ２００の公開鍵を個々に入手する繁雑さが省け、ネットワークトラフィック、特に送受信側コンピュータ２００，３００間にわたってのネットワークトラフィックを減少させることができる。

【００５７】（３）エージェント協調システムにおいて、移動型エージェント間通信を行う場合に、送信側エージェントはエージェント協調機構の協調空間にデータをプールし、他方、受信側エージェントは定期的にエージェント協調機構に問い合わせメッセージを発行して通信を実現する方式がある。このような通信方式に従来の認証処理を適用すると処理が著しく繁雑になり、コスト高になるが、本具体例３を適用した場合には、送信側のエージェントＡ２６０，受信側のエージェントＢ３７０を備えた送信側コンピュータ２００，受信側コンピュータ３００間の認証処理コンピュータ１００がユーザ（送信側コンピュータ２００）の公開鍵を管理するので、上述従来の認証処理を適用した場合に比べて処理が簡単になり、コストが低減する。

【００５８】上述具体例１～３においては、受信側コンピュータは単一であったが、本発明方法は、受信側コンピュータが複数の場合にも適用でき、またより大なる効果も発揮できる。以下、具体例４として、受信側コンピュータが複数であるマルチキャスト通信に本発明方法を適用した場合について説明する。

【００５９】〈具体例４の構成〉図１４は、本発明による認証処理方法の具体例４が適用された通信システムを示すブロック図である。ここでは、認証処理コンピュータとして機能するサーバコンピュータ（以下、認証処理コンピュータという。）１００が、送信側コンピュータ２００とはネットワーク４００によって接続され、複数の、ここでは３つの受信側コンピュータ３００（３００ａ，３００ｂ，３００ｃ）とはネットワーク４０１によって接続されたマルチキャスト通信機能をもつシステムの全体構成を示している。

【００６０】このシステムは図１に示す具体例１と近似するので、各部については図１のシステムとの相違点のみについて述べる。上述したように、ここでは３つの受信側コンピュータ３００ａ，３００ｂ，３００ｃが存在し、各々ネットワーク４０１により認証処理コンピュータ１００に接続されている。各受信側コンピュータ３００ａ，３００ｂ，３００ｃは同一構成である。認証処理コンピュータ１００のアプリケーションサーバプログラ

ム１１０には、図１の認証通信サービス処理部１１１に代えて、マルチキャスト通信機能をもつマルチキャスト認証通信サービス処理部１１１ａが備えられている。ここで、マルチキャスト通信機能とは、送信側コンピュータ２００上のアプリケーションプログラム２１０が認証処理コンピュータ１００に３つの受信側コンピュータ３００ａ，３００ｂ，３００ｃ宛で送信した通信データを、それら３つの受信側コンピュータ３００ａ，３００ｂ，３００ｃに送信する機能をいう。なお図１４において、図１と同一符号は同一又は相当部分を示す。

【００６１】〈具体例４の動作〉次に、上述具体例４の動作について説明する。送信側コンピュータ２００においてアプリケーションプログラム２１０が認証処理コンピュータ１００（アプリケーションサーバプログラム１１０）に通信文を送信する際の当該アプリケーションプログラム２１０の処理は具体例１の場合（図２）と同様である。

【００６２】アプリケーションプログラム２１０が送信する通信文には、受信者情報として３人の受信者を記述する。すなわち、ここでの通信データのフォーマットは図１５に示すようになる。送信者はＡ、受信者はＢ，Ｃ，Ｄで表現されており、Ａ～Ｄは、各アドレス情報を含む。図示するように、通信文は送信者情報Ａ及び受信者情報Ｂ，Ｃ，Ｄと通信文本体とからなり、この通信文と、通信文のメッセージダイジェストのデジタル署名とで通信データが構成される。具体例４では、送信者情報Ａは送信側コンピュータ２００、受信者情報Ｂは受信側コンピュータ３００ａ、受信者情報Ｃは受信側コンピュータ３００ｂ、受信者情報Ｄは受信側コンピュータ３００ｃとなる。

【００６３】送信側コンピュータ２００からの通信データを受信した認証処理コンピュータ１００（アプリケーションサーバプログラム１１０）の動作は図１６に示す通りである。すなわち、アプリケーションサーバプログラム１１０は、まず送信側コンピュータ２００からの通信文とデジタル署名を合わせてなる通信データを受信する（ステップＳ１６１）。

【００６４】次に、アプリケーションサーバプログラム１１０は、デジタル署名検証処理部１１３によって送信側コンピュータ２００のデジタル署名の検証を行う（ステップＳ１６２）。このデジタル署名の検証は、以下の手順で行う。初めに、アプリケーションサーバプログラム１１０は、ユーザ公開鍵データベース１２０に登録されている送信側コンピュータ２００の公開鍵を使用して、送信側コンピュータ２００のデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェスト処理部１１２によって、上記通信文のメッセージダイジェストを新たに生成する。そして、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終了する。不一致であれば送信側コンピュータ２００にエラーを通知する。

【００６５】デジタル署名の検証後、アプリケーションサーバプログラム１１０は、デジタル署名生成処理部１１４を起動し、秘密鍵管理部１３０で管理する自プログラムの秘密鍵を使用して、上記通信文のメッセージダイジェストのデジタル署名を新たに生成する（ステップＳ１６３）。その後、アプリケーションサーバプログラム１１０は、上記通信文と新たに生成したデジタル署名を合わせてなる通信データを受信側コンピュータ３００に送信する（ステップＳ１６４）。

【００６６】通信データの受信側コンピュータ３００への送信（ステップＳ１６４）は受信側コンピュータ３００の数だけ、ここでは受信側コンピュータ３００ａ，３００ｂ，３００ｃの３回繰り返して行われ、マルチキャスト通信が実現される（ステップＳ１６５）。各受信者情報は、上記通信文を参照することによって知り得る。各受信側コンピュータ３００においてアプリケーションプログラム３１０が通信文を受信する際の当該アプリケーションプログラム３１０の処理は具体例１の場合（図５）と同様である。

【００６７】〈具体例４の効果〉

（１）マルチキャスト通信においても、従来技術のように各々が協調して動作する階層構造で組織化された多数の公開鍵認証局ではなく、単一階層構造で独立して動作する認証処理コンピュータ１００が送信側コンピュータ２００の公開鍵を管理するので、送信側コンピュータ２００の公開鍵の運用面で、柔軟で管理しやすいシステムを構築することができる。

【００６８】（２）従来、デジタル署名を使用し複数の受信者間にて相手認証を行う場合、各受信側コンピュータが送信側コンピュータ毎に送信側コンピュータの公開鍵を入手する必要があった。具体例４では、上記認証処理コンピュータ１００がユーザ（送信側コンピュータ２００）の公開鍵をまとめて管理するので、各受信側コンピュータ３００（３００ａ，３００ｂ，３００ｃ）が送信側コンピュータ２００の公開鍵を個々に入手する繁雑さが省け、ネットワークトラフィック、特に送受信側コンピュータ２００，３００間にわたってのネットワークトラフィックを減少させることができる。具体例４におけるこのような効果は、具体例１における二者間の認証通信での効果と比較して、受信側コンピュータ数が増える分、より顕著なものとなる。

【００６９】上述具体例１，４においては、認証処理コンピュータ１００がユーザ公開鍵データベース１２０を備えている。また、具体例２においては、コンピュータ１００がオブジェクト公開鍵データベース１６０を備えている。更に、具体例３においては、エージェント協調機構１７０がエージェント公開鍵データベース１７４を

備えている。これを、ＩＴＵ－Ｘ．５０９等の規格通りに、公開鍵認証局が上記各公開鍵データベースを管理する構成にすることも可能である。以下、具体例５として、具体例１（図１）において、認証処理コンピュータ１００からユーザ公開鍵データベース１２０を除外し、それに代えてＩＴＵ－Ｘ．５０９等の規格による外部の公開鍵認証局を利用する場合について説明する。

【００７０】〈具体例５の構成〉図１７は、本発明による認証処理方法の具体例５が適用された通信システムを示すブロック図である。ここでは、認証処理コンピュータとして機能するサーバコンピュータ（以下、認証処理コンピュータという。）１００が、送信側コンピュータ２００とはネットワーク４００によって、受信側コンピュータ３００とはネットワーク４０１によって、各々接続されたシステムの全体構成を示している。図示するように、本具体例５では、認証処理コンピュータ１００がネットワーク４０４によって外部の公開鍵認証局７００と接続されている。そして、ユーザ（送信側コンピュータ２００）のデジタル署名を検証する際に参照，使用されるユーザ公開鍵データベースとしては、上記公開鍵認証局７００内に備えられ、ＩＴＵ－Ｘ．５０９等の規格通りにその公開鍵認証局７００で管理されているユーザ公開鍵データベース７１０が使用されるようになされている。ユーザの公開鍵は上記ユーザ公開鍵データベース７１０に登録されている。上記ユーザ公開鍵データベース７１０は、デジタル署名の検証時には、アプリケーションサーバプログラム１１０の管理下にある。その他は、具体例１（図１）と同様であるので、図１４において、図１と同一部分に同一符号を付してその説明を省略する。

【００７１】〈具体例５の動作〉次に、上述具体例５の動作について説明する。送信側コンピュータ２００においてアプリケーションプログラム２１０が認証処理コンピュータ１００（アプリケーションサーバプログラム１１０）に通信文を送信する際の当該アプリケーションプログラム２１０の処理は具体例１の場合（図２）と同様である。アプリケーションプログラム２１０が送信する通信データのフォーマットも具体例１の場合（図３）と同様である。

【００７２】送信側コンピュータ２００からの通信データを受信した認証処理コンピュータ１００（アプリケーションサーバプログラム１１０）の動作は図１８に示す通りである。すなわち、アプリケーションサーバプログラム１１０は、まず送信側コンピュータ２００からの通信文とデジタル署名を合わせてなる通信データを受信する（ステップＳ１８１）。

【００７３】次に、アプリケーションサーバプログラム１１０は、公開鍵認証局７００のユーザ公開鍵データベース７１０からユーザ（送信側コンピュータ２００）の公開鍵を取得（ステップＳ１８２）した後、デジタル署名検証処理部１１３によって送信側コンピュータ２００のデジタル署名の検証を行う（ステップＳ１８３）。このデジタル署名の検証は、以下の手順で行う。初めに、アプリケーションサーバプログラム１１０は、ステップ１８２で取得した送信側コンピュータ２００の公開鍵を使用して、送信側コンピュータ２００のデジタル署名からメッセージダイジェストを取り出す。次に、メッセージダイジェスト処理部１１２によって、上記通信文のメッセージダイジェストを新たに生成する。そして、上記デジタル署名から取り出したメッセージダイジェストと新たに生成したメッセージダイジェストとを比較し、それらの一致が確認されればデジタル署名の検証が正常終了する。不一致であれば送信側コンピュータ２００にエラーを通知する。

【００７４】デジタル署名の検証後、アプリケーションサーバプログラム１１０は、デジタル署名生成処理部１１４を起動し、秘密鍵管理部１３０で管理する自プログラムの秘密鍵を使用して、上記通信文のメッセージダイジェストのデジタル署名を新たに生成する（ステップＳ１８４）。その後、アプリケーションサーバプログラム１１０は、上記通信文と新たに生成したデジタル署名を合わせてなる通信データを受信側コンピュータ３００に送信する（ステップＳ１８５）。受信者情報は、上記通信文を参照することによって知り得る。受信側コンピュータ３００においてアプリケーションプログラム３１０が通信文を受信する際の当該アプリケーションプログラム３１０の処理は具体例１の場合（図５）と同様である。

【００７５】〈具体例５の効果〉

（１）従来技術のように各々が協調して動作する階層構造で組織化された多数の公開鍵認証局ではなく、単一階層構造で独立して動作する認証処理コンピュータ１００の管理下において送信側コンピュータ２００の公開鍵を管理するので、送信側コンピュータ２００の公開鍵の運用面で、柔軟で管理しやすいシステムを構築することができる。

【００７６】（２）従来、デジタル署名を使用した二者間の相手認証においては、受信側コンピュータが送信側コンピュータ毎に送信側コンピュータの公開鍵を入手する必要があった。具体例５では、上記認証処理コンピュータ１００がその管理下においてユーザ（送信側コンピュータ２００）の公開鍵をまとめて管理するので、受信側コンピュータ３００が送信側コンピュータ２００の公開鍵を個々に入手する繁雑さが省け、ネットワークトラフィック、特に送受信側コンピュータ２００，３００間にわたってのネットワークトラフィックを減少させることができる。

【００７７】なお、具体例１～５（図１，６，１０，１４，１７）では、いずれも送信側コンピュータ２００と受信側コンピュータ３００とが１対１（具体例４のマル

チキャスト通信の場合は１対１組）の場合を示しているが、実際には送信側コンピュータ２００と受信側コンピュータ３００との組み合わせは認証処理コンピュータ１００を挟んで複数組存在している。各具体例は、いずれもそのように複数組存在している場合にも各組において同様に動作し、同様の効果が得られる。また、具体例１～５において、各公開鍵データベースにおける公開鍵について「管理」とは、当該公開鍵の登録、抹消、更新、検索及び参照等をいう。

【図面の簡単な説明】

【図１】本発明方法の具体例１が適用された通信システムを示すブロック図である。

【図２】図１中の送信側コンピュータにおけるアプリケーションプログラムの動作を示すフローチャートである。

【図３】図１中の認証処理コンピュータのアプリケーションサーバプログラムに送信される通信データのフォーマットの概略を示す図である。

【図４】図１中の認証処理コンピュータにおけるアプリケーションサーバプログラムの動作を示すフローチャートである。

【図５】図１中の受信側コンピュータにおけるアプリケーションプログラムの動作を示すフローチャートである。

【図６】本発明方法の具体例２が適用された通信システムを示すブロック図である。

【図７】図６中の送信側コンピュータにおけるオブジェクトの動作を示すフローチャートである。

【図８】図６中の認証処理コンピュータにおける認証パイプオブジェクトの動作を示すフローチャートである。

【図９】図６中の受信側コンピュータにおけるオブジェクトの動作を示すフローチャートである。

【図１０】本発明方法の具体例３が適用された通信システムを示すブロック図である。

【図１１】図１０中の送信側コンピュータにおけるエージェントの動作を示すフローチャートである。

【図１２】図１０中の認証処理コンピュータにおけるエージェント協調機構の動作を示すフローチャートである。

【図１３】図１０中の受信側コンピュータにおけるエージェントの動作を示すフローチャートである。

【図１４】本発明方法の具体例４が適用された通信システムを示すブロック図である。

【図１５】図１４中の認証処理コンピュータのアプリケーションサーバプログラムに送信される通信データのフォーマットの概略を示す図である。

【図１６】図１４中の認証処理コンピュータにおけるアプリケーションサーバプログラムの動作を示すフローチャートである。

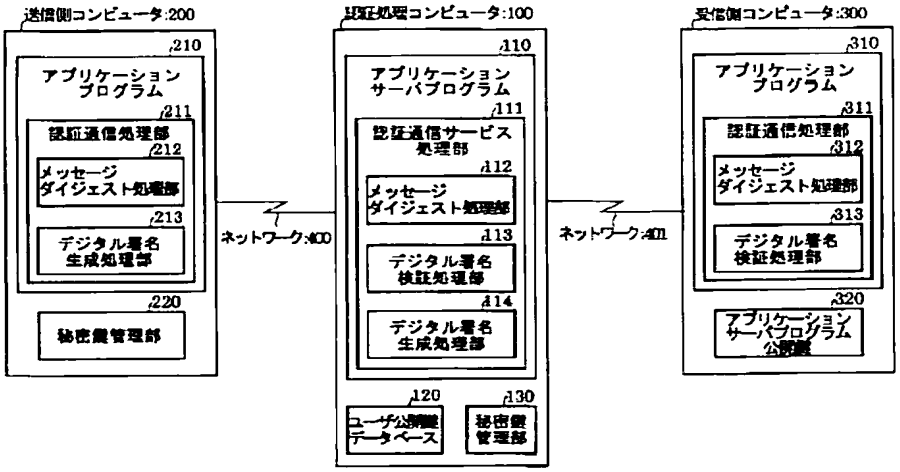
【図１７】本発明方法の具体例５が適用された通信システムを示すブロック図である。

【図１８】図１７中の認証処理コンピュータにおけるアプリケーションサーバプログラムの動作を示すフローチャートである。

【符号の説明】

１００　認証処理コンピュータ
１１０　アプリケーションサーバプログラム
１１１　認証通信サービス処理部
１１２　メッセージダイジェスト処理部
１１３　デジタル署名検証処理部
１１４　デジタル署名生成処理部
１２０　ユーザ公開鍵データベース
１３０　秘密鍵管理部
２００　送信側コンピュータ
２１０　アプリケーションプログラム
２１１　認証通信処理部
２１２　メッセージダイジェスト処理部
２１３　デジタル署名生成処理部
２２０　秘密鍵管理部
３００　受信側コンピュータ
３１０　アプリケーションプログラム
３１１　認証通信処理部
３１２　メッセージダイジェスト処理部
３１３　デジタル署名検証処理部
３２０　アプリケーションサーバプログラム公開鍵
４００，４０１　ネットワーク

【図１】



具体例１のシステム構成図

【図２】

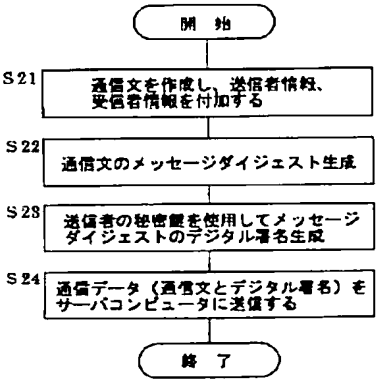


図１中の送信側コンピュータの動作フローチャート

【図３】

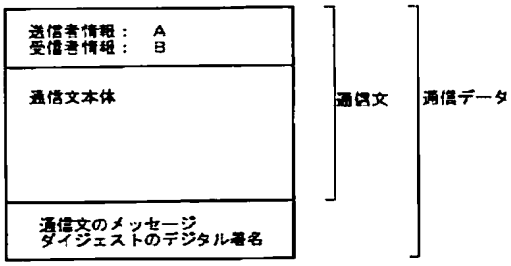


図１中の認証処理コンピュータへの通信データのフォーマット概略図

【図４】

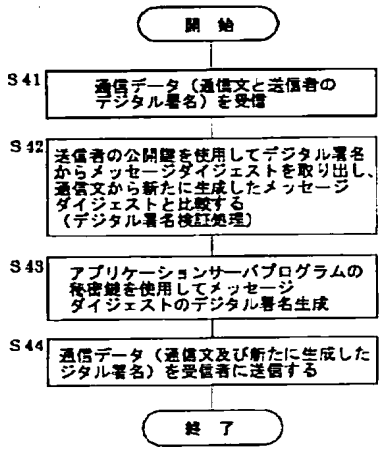


図１中の認証処理コンピュータの動作フローチャート

【図５】

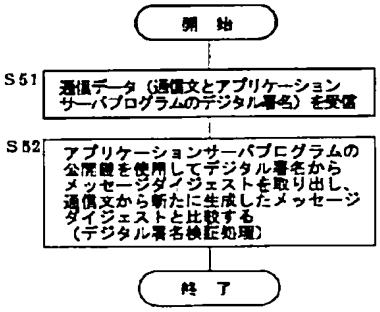


図１中の受信側コンピュータの動作フローチャート

【図９】

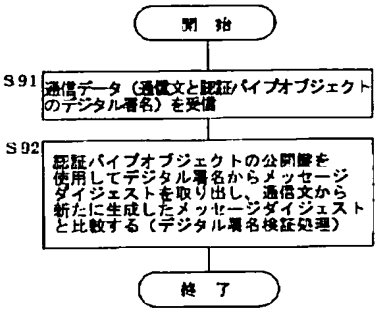
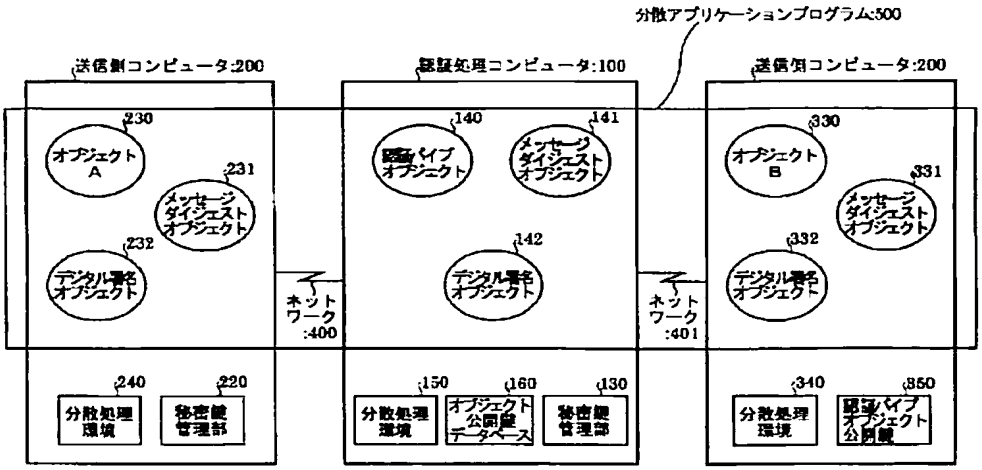


図６中の受信側コンピュータの動作フローチャート

【図６】



具体例２のシステム構成図

【図７】

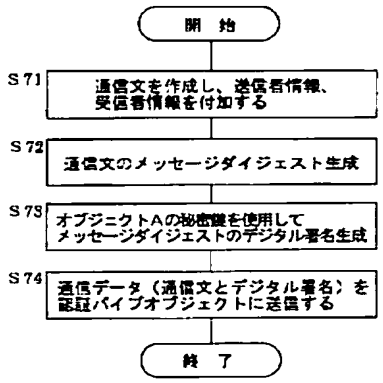


図６中の送信側コンピュータの動作フローチャート

【図８】

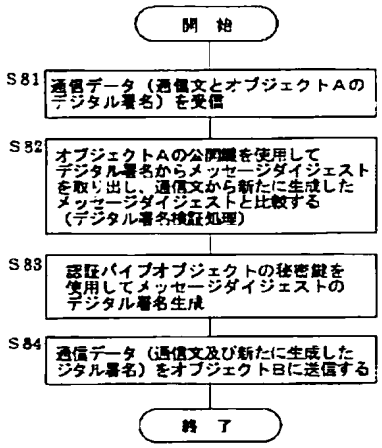


図６中の認証処理コンピュータの動作フローチャート

【図１５】

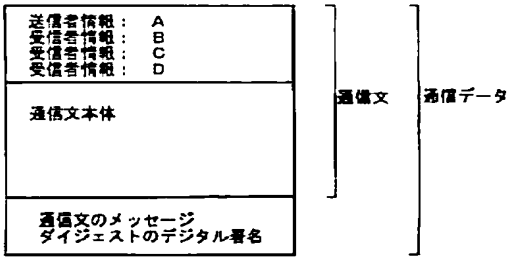
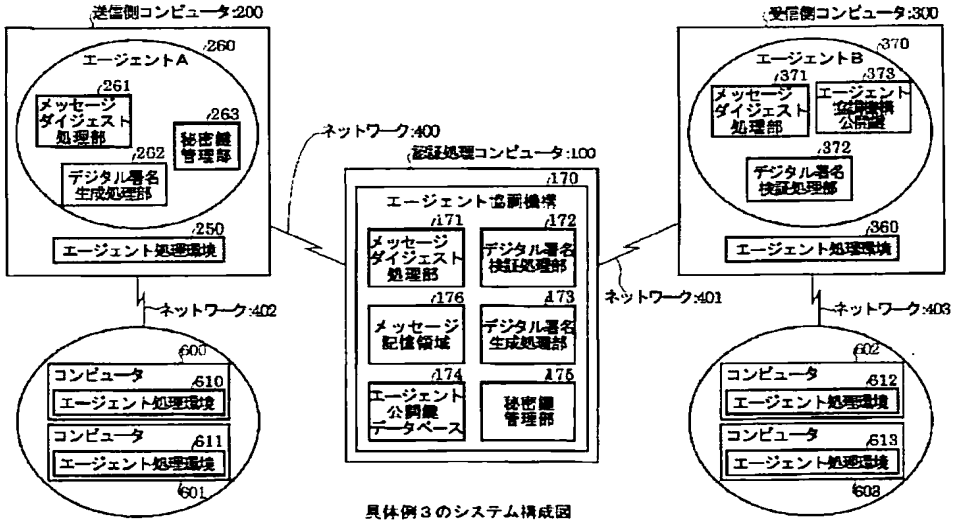


図１４中の認証処理コンピュータへの通信データのフォーマット概略図

【図１０】



具体例３のシステム構成図

【図１１】

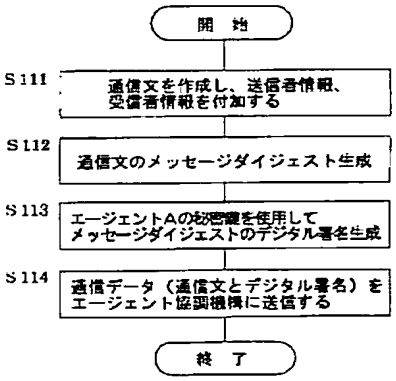


図１０中の送信側コンピュータの動作フローチャート

【図１２】

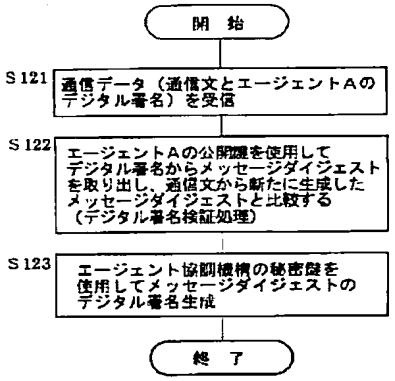


図１０中の認証処理コンピュータの動作フローチャート

【図１３】

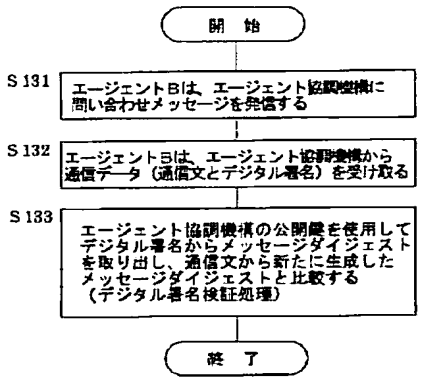
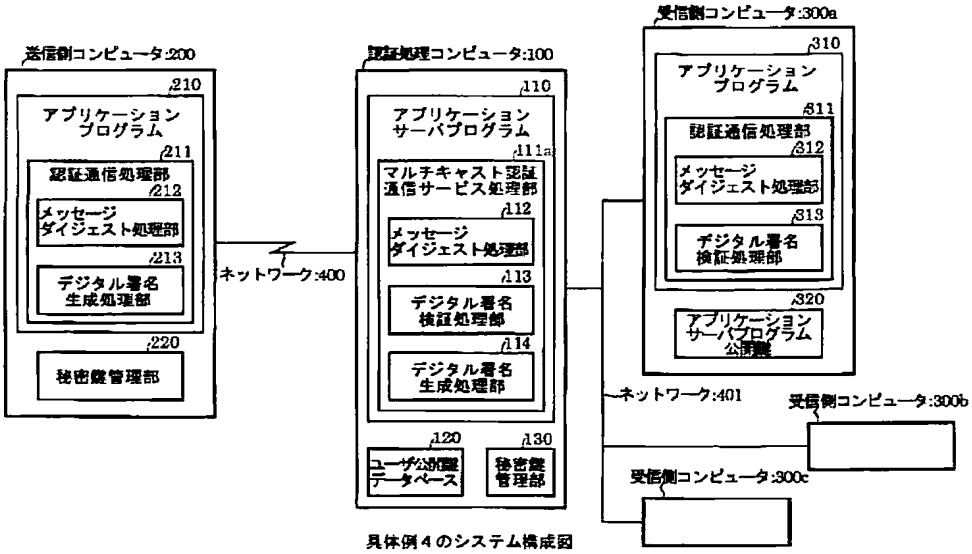


図１０中の受信側コンピュータの動作フローチャート

【図１４】



具体例４のシステム構成図

【図１６】

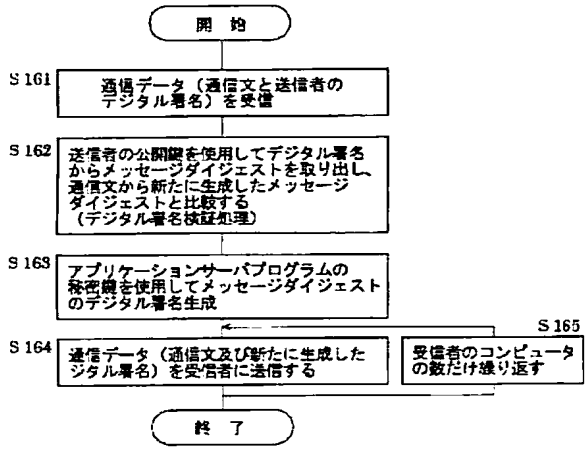


図１４中の認証処理コンピュータの動作フローチャート

【図１８】

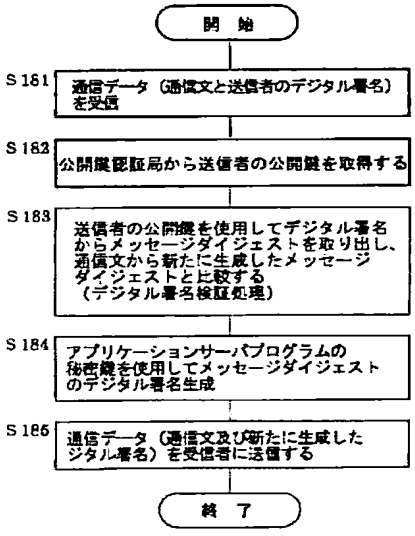
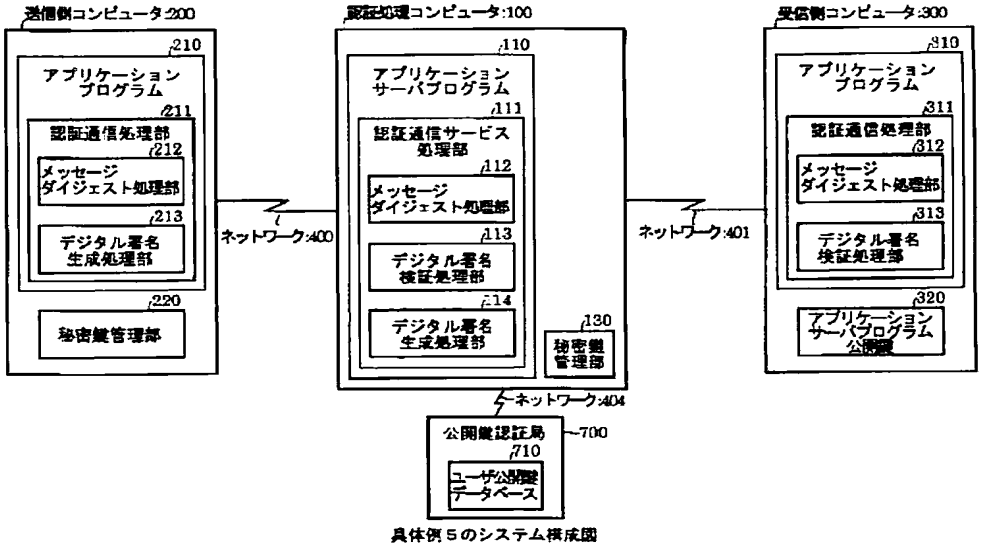


図１７中の認証処理コンピュータの動作フローチャート

【図１７】



具体例５のシステム構成図

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-138670

(43)Date of publication of application : 16.05.2000

(51)Int.Cl. H04L 9/32

G09C 1/00

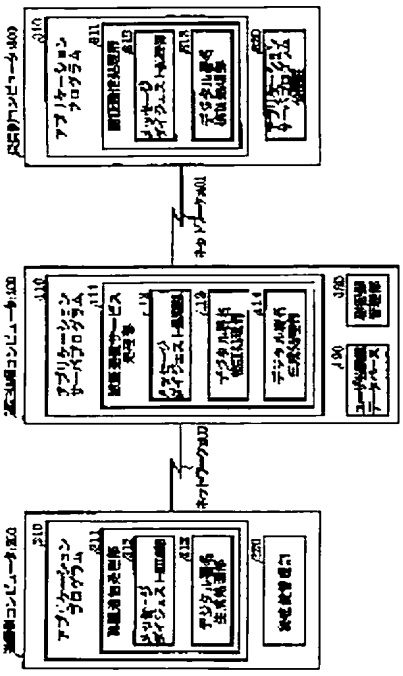
(21)Application number : 10-309713

(22)Date of filing : 30.10.1998

(71)Applicant : OKI ELECTRIC IND CO LTD

(72)Inventor : KOYAMA NORITAKA

(54) AUTHENTICATION PROCESSING METHOD



(57)Abstract:

PROBLEM TO BE SOLVED: To authenticate a transmission side computer between the computer on the transmission side and a computer on a receiving side by allowing the computer on the receiving side to execute inspection in the computer on the receiving side, after receiving an open key from an authentication processing computer.

SOLUTION: An application server program 110 receives communication data composed of a communication message and a digital signature from the computer on the transmission side 200. The program 110 fetches a message digest from the digital signature of the computer 200. Next, a message digest processing part 112 generates the message digest of the communication message from an application program 210 and compares it with the fetched from the digital signature. After inspection, the digital signature of the message digest is generated by using a secret key and communication data composed with the communication message is transmitted to the computer on the

receiving side 300.

LEGAL STATUS

[Date of request for examination] 27.12.2001

[Date of sending the examiner's decision of rejection] 09.11.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The transmitting-side computer which generates a digital signature using a self private key to the fixed-length message digest taken out from the correspondence of arbitration, adds to said correspondence, and is transmitted to a network as commo data, A message digest is taken out from the digital signature in

the commo data from said network using a public key. In the communication system to which the receiving–side computer which can perform the verification as compared with the message digest newly generated from the correspondence in the commo data from this network in it was connected through said network The authentication processing computer which was formed between said transmitting–side computer and the receiving–side computer and which operates independently by the single layered structure Receive the commo data from said transmitting–side computer, and a message digest is taken out from the digital signature in the commo data from a transmitting–side computer using the public key of the transmitting–side computer registered into the public key database under self management. The verification is performed as compared with the message digest newly generated from the correspondence in the commo data from a transmitting–side computer in it. After the check of those coincidence, newly generate a digital signature using a self private key from a message digest, add to the correspondence in the commo data from said transmitting–side computer, and it transmits to said receiving–side computer as commo data. The authentication art to which said receiving–side computer is characterized by attesting the transmitting–side computer between said transmitting–side computer and a receiving–side computer by performing said verification in that receiving–side computer in response to that public key from this authentication processing computer.

[Claim 2] It is the authentication art characterized by being the computer which a transmitting–side computer, a receiving–side computer, and an authentication processing computer mount a distributed–processing environment respectively in an authentication art according to claim 1, and performs distributed processing.

[Claim 3] It is the authentication art characterized by being the computer which constitutes the agent coordination system by which the transmitting–side computer and the receiving–side computer mounted the agent processing environment, and, as for the transmitting–side computer, the receiving–side computer, and the authentication processing computer, the authentication processing computer mounted the agent coordination device respectively in the authentication art according to claim 1.

[Claim 4] It is the authentication art characterized by being the multicast communication link in which, as for the communication link between computers by the side of transmission and reception, two or more computers of a receiving side exist in an authentication art according to claim 1, 2, or 3.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the authentication art which performs partner authentication using a digital signature, and relates to the suitable authentication art for partner authentication by the electronic mail in the Internet or intranet, electronic banking, or the agent coordination system especially.
[0002]
[Description of the Prior Art] him who is represented by a signature and seal stamp — it is for realizing authentication (if it seeing from a sink partner authentication) on online media, such as a communication network. [in / in a digital signature / dealings in the paper base] Partner authentication which used the digital signature is performed as follows. That is, the transmitting person of Correspondence x transmits the digital signature Sig (Ks, x) generated from the above-mentioned correspondence x with the digital signature generation algorithm which used a transmitting person's private key (key which only he gets to know) Ks. An addressee processes a digital signature Sig (Ks, x) with the digital signature verification algorithm which used a transmitting person's public key (said private key Ks and key with which a pair can be known also except nothing and a transmitting person) Kp, and performs partner authentication by verifying "Ver(Kp, Sig (Ks, x)) =x."
[0003] Generation processing of a digital signature is used together with message digest processing in fact in many cases. It is because generation of the digital signature Sig (Ks, x) from the long sentence x takes time amount so much and it becomes cost quantity. Here, the processing to which message digest processing generates fixed-length about 100-160 bits, for example, 128 bits, message digest M

(x) to Correspondence x in the original sentence of arbitration length and the above-mentioned example is said.

[0004] In this case, a transmitting person generates the digital signature Sig (Ks, M (x)) to the above message digest M (x) using the above-mentioned private key Ks, and transmits this together with the above-mentioned correspondence x. An addressee generates himself new message digest M (x) from the sent correspondence x, and verifies "Ver(Kp, Sig (Ks, M (x))) =M (x)." That is, an addressee generates message digest M (x) from the above-mentioned digital signature Sig (Ks, M (x)) using a transmitting person's public key Kp. Partner authentication is performed by comparing with new message digest M (x) itself generated by the same technique with the transmitting person having carried out from the correspondence x to which this has been sent together with the above-mentioned digital signature Sig (Ks, M (x)). If the above-mentioned comparison result comes out with "coincidence", a transmitting person's digital signature will be checked as it is a genuine article (partner authentication), and, specifically, the integrity (there do not need to be data corruption and an alteration) of correspondence will be checked.

[0005] As mentioned above, when an addressee verifies a transmitting person's digital signature, it is necessary to use a transmitting person's public key. In the application of the former many, he is for an addressee to receive the public key certificate with which the digital signature of a reliable public key certificate authority was given, to verify the digital signature of a certificate authority, and to use a transmitting person's public key (ITU-X.509 (Internation Telecommunication Union X series recommendation 509)). On the other hand, a transmitting person can also transmit a public key certificate and each hierarchized public key certificate of a public key certificate authority which is mentioned later with correspondence. In this case, an addressee needs to receive a public key certificate lapse list from a reliable public key certificate authority, in order to check whether those public key certificates are invalidated. Therefore, when the addressee needs acquisition of a public key and a transmitting person transmits hereafter including a public key certificate, acquisition of a public key certificate lapse list shall be demanded of coincidence.

[0006]

[Problem(s) to be Solved by the Invention] However, there were the following troubles in the above-mentioned conventional technique.

(1) It is systematized by the layered structure, each certificate authority cooperates, and the public key certificate authority specified in the ITU-X.509 grade for employment of the public key used by verification of a digital signature and

management operates. However, when this structure managed the database of a public key certificate by many certificate authorities of a layered structure, it held difficulty in maintenance of that coordination, especially maintenance of the identity of each certificate authority in cancellation and an update process of a public key certificate and the demand of that quick nature was moreover also considered, it had the trouble of the flexibility in increase, consequently the aspect of practical use of a public key having been lost, and being much more hard to manage difficulty.

[0007] (2) In the partner authentication between the 2 persons who used the digital signature, the addressee needed to receive a transmitting person's public key for every transmitting person, and public key acquisition processing became complicated, and there was a trouble of network traffic increasing.

[0008] (3) In an agent coordination system, when performing the communication link between migration mold agents, a transmitting-side agent pools data to the coordination space of an agent coordination device, and another side and a receiving-side agent have the method which asks periodically an agent coordination device, publishes a message, and realizes a communication link. In such a communication mode, with each agent, when it became complicated, therefore authentication processing of the above-mentioned former was applied to such a communication mode, succession and the trouble that processing became remarkably complicated and became cost quantity had the communication link between agent coordination devices.

[0009] (4) When the partner authentication which used the digital signature was applied to a multicast communication link, each addressee needed to receive a transmitting person's public key respectively, and public key acquisition processing became complicated, and there was a trouble of network traffic increasing.

[0010] This invention is made that the trouble of the above-mentioned conventional technique should be canceled.

[0011]

[Means for Solving the Problem] The next configuration is used for this invention in order to solve the above-mentioned technical problem.

<Configuration 1> The transmitting-side computer which generates a digital signature using a self private key to the fixed-length message digest taken out from the correspondence of arbitration, adds to the above-mentioned correspondence, and is transmitted to a network as commo data, A message digest is taken out from the digital signature in the commo data from the above-mentioned network using a public key. In the communication system to which the receiving-side computer which can

perform the verification as compared with the message digest newly generated from the correspondence in the commo data from this network in it was connected through the above-mentioned network The authentication processing computer which was formed between the above-mentioned transmitting-side computer and the receiving-side computer and which operates independently by the single layered structure Receive the commo data from the above-mentioned transmitting-side computer, and a message digest is taken out from the digital signature in the commo data from a transmitting-side computer using the public key of the transmitting-side computer registered into the public key database under self management. The verification is performed as compared with the message digest newly generated from the correspondence in the commo data from a transmitting-side computer in it. After the check of those coincidence, newly generate a digital signature using a self private key from a message digest, add to the correspondence in the commo data from the above-mentioned transmitting-side computer, and it transmits to the above-mentioned receiving-side computer as commo data. The authentication art to which the above-mentioned receiving-side computer is characterized by attesting the transmitting-side computer between the above-mentioned transmitting-side computer and a receiving-side computer by performing the above-mentioned verification in that receiving-side computer in response to that public key from this authentication processing computer.

[0012] <Configuration 2> It is the authentication art characterized by being the computer which a transmitting-side computer, a receiving-side computer, and an authentication processing computer mount a distributed-processing environment respectively in an authentication art according to claim 1, and performs distributed processing.

[0013] <Configuration 3> It is the authentication art characterized by being the computer which constitutes the agent coordination system by which the transmitting-side computer and the receiving-side computer mounted the agent processing environment, and, as for the transmitting-side computer, the receiving-side computer, and the authentication processing computer, the authentication processing computer mounted the agent coordination device respectively in the authentication art according to claim 1.

[0014] <Configuration 4> It is the authentication art characterized by being the multicast communication link in which, as for the communication link between computers by the side of transmission and reception, two or more computers of a receiving side exist in an authentication art according to claim 1, 2, or 3.

[0015]

[Embodiment of the Invention] Hereafter, it explains using a drawing per gestalt of operation of this invention.

<<example>>

<Configuration of an example 1> Drawing 1 is the block diagram showing the communication system with which the example 1 of the authentication art by this invention was applied. Here, the whole system configuration to which the server computer (henceforth an authentication processing computer) 100 which functions as an authentication processing computer was connected to by the network 400 in the transmitting-side computer 200, and was respectively connected by the network 401 in the receiving-side computer 300 is shown.

[0016] The above-mentioned authentication processing computer 100 operates independently by the single layered structure, and comes to have the application server program 110, the user public key database 120, and the private key Management Department 130. Here, the application server program 110 is equipped with the message digest processing section 112, the digital signature verification processing section 113, and the authentication communication service processing section 111 that consists of digital signature generation processing section 114 grade. The user public key database 120 is a database which registered a user's (transmitting-side computer 200) public key, and in case it is under management of the application server program 110 and verifies a user's digital signature, it is used. The private key Management Department 130 manages the private key of the application server program 110 used in case a digital signature is generated in the authentication processing computer 100.

[0017] The transmitting-side computer 200 comes to have an application program 210 and the private key Management Department 220. Here, an application program 210 is equipped with the authentication communications processing section 211 which consists of the message digest processing section 212 and digital signature generation processing section 213 grade. The private key Management Department 220 manages the private key of the transmitting-side computer 200 used in case the digital signature of the transmitting-side computer 200 is generated.

[0018] The receiving-side computer 300 comes to have an application program 310 and the application server program public key 320. Here, an application program 310 is equipped with the authentication communications processing section 311 which consists of the message digest processing section 312 and digital signature verification processing section 313 grade. The application server program public key

320 is used in case a digital signature is verified.

[0019] <Actuation of an example 1> Next, actuation of the above-mentioned example 1 is explained. Drawing 2 is a flow chart which shows actuation of the application program 210 in the transmitting-side computer 200. As shown in this drawing, an application program 210 creates the body of correspondence first, and adds transmitting person information and recipient information in the format beforehand decided to be it (step S21). Hereafter, what added those information to the correspondence body is called correspondence.

[0020] Next, an application program 210 generates the digital signature to the above-mentioned message digest using the private key of the transmitting-side computer 200 and the digital signature generation processing section 213 which generated the message digest of correspondence using the message digest processing section 212 (step S22), then have been managed at the private key Management Department 220 (step S23). Then, the commo data with which it comes to double the above-mentioned correspondence and a digital signature is transmitted to the authentication processing computer 100 (application server program 110) (step S24), and the correspondence transmitting procedure in the transmitting-side computer 200 is ended.

[0021] The outline of a format of the data (commo data) transmitted to the above-mentioned application server program 110 at drawing 3 is shown. Here, a transmitting person is expressed by A, the addressee is expressed by B, and A and B contain each address information. Correspondence consists of the transmitting person information A and recipient information B, and a correspondence body so that it may illustrate, and it is the digital signature (a message digest is included.) of the message digest of this correspondence and correspondence. this specification -- setting -- the same . Commo data is constituted. In the transmitting person information A, by the example 1, the transmitting-side computer 200 and recipient information B serve as the receiving-side computer 300.

[0022] Drawing 4 is a flow chart which shows actuation of the application server program 110 in the authentication processing computer 100. As shown in this drawing, the application server program 110 (authentication processing computer 100) receives the commo data (refer to drawing 3) which doubles the correspondence and the digital signature from the transmitting-side computer 200 first, and becomes (step S41).

[0023] Next, the application server program 110 verifies the digital signature of the transmitting-side computer 200 by the digital signature verification processing

section 113 (step S42). The digital signature verification processing section 113 performs verification of this digital signature in the following procedures. Introduction and the application server program 110 use the public key of the transmitting-side computer 200 (user) registered into the user public key database 120, and take out a message digest from the digital signature of the transmitting-side computer 200. Next, the message digest processing section 112 newly generates the message digest of the correspondence from an application program 210. And the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest, and if those coincidence is checked, verification of a digital signature will terminate normally. If inharmonious, an error will be notified to the transmitting-side computer 200.

[0024] After verification of a digital signature, the application server program 110 starts the digital signature generation processing section 114, uses the private key of the self-program managed at the private key Management Department 130, and newly generates the digital signature of the message digest of the above-mentioned correspondence (step S43). Then, the application server program 110 transmits the commo data with which it comes to double the digital signature newly generated at the above-mentioned correspondence and step 43 to the receiving-side computer 300 (step S44). Recipient information can be known by referring to the above-mentioned correspondence.

[0025] Drawing 5 is a flow chart which shows actuation of the application program 310 in the receiving-side computer 300. First, the application program 310 on the receiving-side computer 300 receives the commo data with which it comes to double the correspondence from the authentication processing computer 100 (application server program 110), and a new digital signature (digital signature by the application server program 110) (step S51).

[0026] Next, an application program 310 verifies the new digital signature from the authentication processing computer 100 (step S52). The digital signature verification processing section 313 performs verification of this digital signature in the following procedures. The application server program public key 320 is used for introduction and an application program 310, and they take out a message digest from the digital signature from the application server program 110. Next, the message digest processing section 312 newly generates the message digest of the correspondence from the application server program 110. And the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest, and if those coincidence is checked, verification of a digital signature will

terminate normally. Normal termination of verification terminates the authentication communications processing from the transmitting-side computer 200 to the receiving-side computer 300.

[0027] <Effectiveness of an example 1> Since the authentication processing computer 100 by which it operates independently by not a public key certificate authority but the single layered structure of a large number systematized by the layered structure as for which each operates in cooperation manages the public key of the transmitting-side computer 200 like (1) conventional technique, the system which it is flexible and is easy to manage on the aspect of practical use of the public key of the transmitting-side computer 200 can be built.

[0028] (2) In the partner authentication between the 2 persons who used the digital signature, the receiving-side computer needed to receive the public key of a transmitting-side computer for every transmitting-side computer conventionally. By the example 1, since the above-mentioned authentication processing computer 100 manages a user's (transmitting-side computer 200) public key collectively, the complicatedness to which the receiving-side computer 300 receives the public key of the transmitting-side computer 200 separately can be excluded, and network traffic, especially the network traffic covering between the transmission-and-reception side computers 200,300 can be decreased.

[0029] <Configuration of an example 2> Drawing 6 is the block diagram showing the communication system with which the example 2 of the authentication art by this invention was applied. Here, a computer 200 and a computer 100 are connected by the network 400, a computer 100 and a computer 300 are respectively connected by the network 401, and three computers 100,200,300 which mount the distributed-processing environment 150,240,340 show the whole system configuration in which the distributed application program 500 operates ranging over these three computers 100 and 200 and a computer 300. Based on each function in this example 2, the computer which becomes 100 about three computers 100,200,300 is hereafter called authentication processing computer, and the computer which becomes 200 is called a transmitting-side computer and receiving-side computer which becomes 300.

[0030] The above-mentioned authentication processing computer 100 is equipped with the authentication pipe object 140, the message digest object 141 and the digital signature object 142 which operate independently by the single layered structure and operate with the above-mentioned distributed application program 500 besides the above-mentioned distributed-processing environment 150, the private key Management Department 130 which manages the private key of the authentication

pipe object 140, and the object public key database 160 with which the public key of all the objects in an illustration system (user) was registered. This object public key database 160 is used, in case it is under management of the authentication pipe object 140 and a user's digital signature is verified.

[0031] The transmitting-side computer 200 is equipped with the object A230, the message digest object 231 and the digital signature object 232 which operate with the above-mentioned distributed application program 500 besides the above-mentioned distributed-processing environment 240, and the private key Management Department 220 which manages the private key of an object A230.

[0032] The receiving-side computer 300 is equipped with the object B330, the message digest object 331 and the digital signature object 332 which operate with the above-mentioned distributed application program 500 besides the above-mentioned distributed-processing environment 340, and the authentication pipe object public key 350.

[0033] In addition, the above-mentioned authentication pipe object 140, an object A230, and an object B330 can have means of communications, and can communicate mutually. Moreover, the message digest object 141,231,331 shall have a message digest generation method respectively, and the digital signature object 142,232,332 shall have a signature verification method and a signature generation method respectively.

[0034] <Actuation of an example 2> Next, actuation of the above-mentioned example 2 is explained. Drawing 7 is a flow chart which shows actuation of the object A230 in the transmitting-side computer 200. As shown in this drawing, an object A230 creates the body of correspondence first, and adds transmitting-side computer 200 (object A230) information and receiving-side computer 300 (object B330) information in the format beforehand decided to be it (step S71). Hereafter, what added those information to the correspondence body is called correspondence.

[0035] Next, an object A230 generates the digital signature to the above-mentioned message digest using the signature generation method of the private key of the object A230 which generated the message digest of correspondence using the message digest generation method of the message digest object 231 (step S72), then has been managed at the private key Management Department 220, and the digital signature object 232 (step S73). Then, the commo data with which it comes to double the above-mentioned correspondence and a digital signature is transmitted to the authentication pipe object 140 on the authentication processing computer 100 (step S74), and the correspondence transmitting procedure of an object A230 is ended. The

format of commo data is the same as that of drawing 3 except for a transmitting person becoming an object A230 and an addressee becoming an object B330.

[0036] Drawing 8 is a flow chart which shows actuation of the authentication pipe object 140 in the authentication processing computer 100. As shown in this drawing, the authentication pipe object 140 receives the commo data which doubles the digital signature of the correspondence from the transmitting-side computer 200 (object A230), and an object A230 first, and becomes (step S81).

[0037] Next, the authentication pipe object 140 verifies the digital signature of an object A230 (step S82). The following procedures perform verification of this digital signature. Introduction and the authentication pipe object 140 use the public key of the object A230 registered into the object public key database 160, and take out a message digest from the digital signature of an object A230. Next, the message digest generation method of the message digest object 141 is used, and the message digest of the above-mentioned correspondence is newly generated. And the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest, and if those coincidence is checked, verification of a digital signature will terminate normally. If inharmonious, an error will be notified to the transmitting-side computer 200.

[0038] After verification of a digital signature, by the signature generation method of the digital signature object 142, the authentication pipe object 140 uses the private key of the self-object managed at the private key Management Department 130, and newly generates the digital signature of the message digest of the above-mentioned correspondence (step S83). Then, the authentication pipe object 140 transmits the commo data with which it comes to double the above-mentioned correspondence and the newly generated digital signature to an object B330 (step S84). Recipient information can be known by referring to the above-mentioned correspondence.

[0039] Drawing 9 is a flow chart which shows actuation of the object B330 in the receiving-side computer 300. First, the object B330 on the receiving-side computer 300 receives the commo data with which it comes to double the correspondence from the authentication processing computer 100 (authentication pipe object 140), and a new digital signature (digital signature by the authentication pipe object 140) (step S91).

[0040] Next, an object B330 verifies the new digital signature from the authentication processing computer 100 (step S92). The following procedures perform verification of this digital signature. Introduction and an object B330 use the authentication pipe object public key 350, and take out a message digest from the digital signature of the

authentication pipe object 140. Next, the message digest generation method of the message digest object 331 is used, and the message digest of the above-mentioned correspondence is newly generated. And the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest, and if those coincidence is checked, verification of a digital signature will terminate normally. Normal termination of verification terminates the authentication communications processing from an object A230 to an object B330.

[0041] <Effectiveness of an example 2> Also in (1) distributed processing system, since the authentication processing computer 100 by which it operates independently by not a public key certificate authority but the single layered structure of a large number systematized by the layered structure as for which each operates in cooperation manages the public key of the transmitting-side computer 200 like the conventional technique, the system which it is flexible and is easy to manage on the aspect of practical use of the public key of the transmitting-side computer 200 can be built.

[0042] (2) In the partner authentication between the 2 persons who used the digital signature in the system which performs distributed processing, the receiving-side computer (object) needed to receive the public key of a transmitting-side computer to every transmitting-side computer (object) conventionally. By the example 2, since the authentication processing computer 100 between the transmitting-side computer 200 equipped with the object A230 which communicates mutually, and the object B330, and the receiving-side computer 300 manages a user's (transmitting-side computer 200) public key collectively. the complicatedness to which the receiving-side computer 300 receives the public key of the transmitting-side computer 200 separately can be excluded, and network traffic, especially the network traffic covering between the transmission-and-reception side computers 200,300 can be decreased.

[0043] <Configuration of an example 3> Drawing 10 is the block diagram showing the communication system with which the example 3 of the authentication art by this invention was applied. Here, the computer 100 which mounts two or more computers 200, 300, and 600,601,602,603 and agent coordination devices 170 which the agent processing environments 250, 360, and 610,611,612,613 are mounted shows the whole agent coordination system configuration connected by the network 400,401,402,403. Based on each function in this example 3, the computer which becomes 100 about a computer 100,200,300 is hereafter called authentication processing computer, and the computer which becomes 200 is called a transmitting-side computer and

receiving-side computer which becomes 300.

[0044] The above-mentioned authentication processing computer 100 operates independently by the single layered structure, and is equipped with the agent coordination device 170. This agent coordination device 170 comes to have the message digest processing section 171, the digital signature verification processing section 172, the digital signature generation processing section 173, the agent public key database 174, the private key Management Department 175, and the message storage region 176. The public key of all the agents in an illustration system (user) is registered into the above-mentioned agent public key database 174. This agent public key database 174 is used, in case it is under management of the agent coordination device 170 and a user's digital signature is verified. The private key Management Department 175 manages the private key of the agent coordination device 170. The message storage region 176 stores temporarily correspondence, a digital signature, etc. from a transmitting-side agent to a receiving-side agent.

[0045] The transmitting-side computer 200 is equipped with the agent A260 besides the above-mentioned agent processing environment 250. Here, an agent A260 comes to have the message digest processing section 261, the digital signature generation processing section 262, and the private key Management Department 263. The private key Management Department 263 manages an agent's A260 private key.

[0046] The receiving-side computer 300 is equipped with the agent B370 besides the above-mentioned agent processing environment 360. Here, an agent B370 comes to have the message digest processing section 371, the digital signature verification processing section 372, and the agent coordination device public key 373.

[0047] The agent of an illustration system may be whichever of the resident mold agent who resides permanently on a migration mold agent with the capacity which moves between two or more computers which mount the agent processing environment, or one computer. Moreover, each agent of an illustration system can have means of communications, and can communicate mutually. When two agents are migration mold agents, they are made possible by the communication link as follows. Here, the migration mold agent who may communicate decides to ask periodically the agent coordination device 170 and to send a message. A transmitting-side agent posts transmit data for the agent coordination device 170, and when a receiving-side agent asks the agent coordination device 170 and sends a message, he gets to know existence of the transmit data addressed to a self-agent, and is made as [obtain / it]. As mentioned above, the agent A260 and agent B370 of an illustration system may be a migration mold, or may be a resident mold, but when it is both a migration mold, they

shall be made possible by the communication link by the above correspondence procedures.

[0048] <Actuation of an example 3> Next, actuation of the above-mentioned example 3 is explained. Drawing 11 is a flow chart which shows the actuation of an agent A260 in the transmitting-side computer 200. As shown in this drawing, an agent A260 creates the body of correspondence first, and adds transmitting-side computer 200 (agent A260) information and receiving-side computer 300 (agent B370) information in the format beforehand decided to be it (step S111). Hereafter, what added those information to the correspondence body is called correspondence.

[0049] Next, an agent A260 generates the digital signature to the above-mentioned message digest using the private key of the agent A260 who generated the message digest of correspondence using the message digest processing section 261 (step S112), then has managed at the private key Management Department 263, and the digital signature generation processing section 262 (step S113). Then, the commo data with which it comes to double the above-mentioned correspondence and a digital signature is transmitted to the agent coordination device 170 on the authentication processing computer 100 (step S114), and an agent's A260 correspondence transmitting procedure is ended. The format of commo data is the same as that of drawing 3 except for transmitting person information becoming an agent A260, and recipient information becoming an agent B370.

[0050] Drawing 12 is a flow chart which shows actuation of the agent coordination device 170 in the authentication processing computer 100. As shown in this drawing, the agent coordination device 170 receives the commo data which doubles the digital signature of the correspondence from the agent A260 on the transmitting-side computer 200, and an agent A260 first, and becomes (step S121).

[0051] Next, the agent coordination device 170 verifies an agent's A260 digital signature by the message digest processing section 171 and the digital signature verification processing section 172 (step S122). The following procedures perform verification of this digital signature. An agent's A260 public key registered into the agent public key database 174 is used for introduction and the agent coordination device 170, and they take out a message digest from an agent's A260 digital signature. Next, the message digest processing section 171 newly generates the message digest of the above-mentioned correspondence. And the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest, and if those coincidence is checked, verification of a digital signature will terminate normally. It will leave the error log, if inharmonious, and when it next asks

from an agent A260 and a message is received, the agent A260 is notified of an error.
[0052] After verification of a digital signature, the agent coordination device 170 starts the digital signature generation processing section 173, and the private key of the agent coordination device 170 managed at the private key Management Department 175 is used for it, and it newly generates the digital signature of the message digest of the above-mentioned correspondence (step S123). The above-mentioned correspondence and the newly generated digital signature are held to the message storage region 176 within the agent coordination device 170.
[0053] Drawing 13 is a flow chart which shows the actuation of an agent B370 in the receiving-side computer 300. First, the agent B370 on the receiving-side computer 300 asks the agent coordination device 170, and sends a message (step 131). On the other hand, the agent coordination device 170 reads the commo data with which it comes to double the correspondence which had already received from the agent A260, and the newly generated digital signature (digital signature by the agent coordination device 170) from the message storage region 176, and passes it to an agent B370 (step 132). (an agent B370 receives the read commo data)
[0054] Next, an agent B370 verifies the new digital signature from the agent coordination device 170 (step S133). The digital signature verification processing section 372 performs verification of this digital signature in the following procedures. Introduction and an agent B370 use the agent coordination device public key 373, and take out a message digest from the digital signature from the agent coordination device 170. Next, the message digest processing section 371 newly generates the message digest of the correspondence from the agent coordination device 170. And if the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest and those coincidence is checked by the digital signature verification processing section 372, verification of a digital signature will terminate normally. Normal termination of verification terminates the authentication communications processing from an agent A260 to an agent B370.
[0055] <Effectiveness of an example 3> Also in (1) agent coordination system, since the authentication processing computer 100 by which it operates independently by not a public key certificate authority but the single layered structure of a large number systematized by the layered structure as for which each operates in cooperation manages the public key of the transmitting-side computer 200 like the conventional technique, the system which it is flexible and is easy to manage on the aspect of practical use of the public key of the transmitting-side computer 200 can be built.

[0056] (2) In the partner authentication between the 2 persons who used the digital signature in an agent coordination system, the receiving-side computer (agent) needed to receive the public key of a transmitting-side computer to every transmitting-side computer (agent) conventionally. By the example 3, since the authentication processing computer 100 between the transmitting-side computer 200 equipped with the agent A260 who communicates mutually, and the agent B370, and the receiving-side computer 300 manages a user's (transmitting-side computer 200) public key collectively, the complicatedness to which the receiving-side computer 300 receives the public key of the transmitting-side computer 200 separately can be excluded, and network traffic, especially the network traffic covering between the transmission-and-reception side computers 200,300 can be decreased.

[0057] (3) In an agent coordination system, when performing the communication link between migration mold agents, a transmitting-side agent pools data to the coordination space of an agent coordination device, and another side and a receiving-side agent have the method which asks periodically an agent coordination device, publishes a message, and realizes a communication link. If the conventional authentication processing is applied to such a communication mode, processing will become remarkably complicated and will become cost quantity, but since the authentication processing computer 100 between the transmitting-side computer 200 equipped with the agent A260 of a transmitting side and the agent B370 of a receiving side and the receiving-side computer 300 manages a user's (transmitting-side computer 200) public key when this example 3 is applied, compared with the case where authentication processing of the above-mentioned former is applied, processing becomes easy, and cost decreases.

[0058] In the above-mentioned examples 1-3, although the receiving-side computer was single, the effectiveness which can apply this invention approach also when a receiving-side computer is plurality, and becomes size more can also be demonstrated. The case where this invention approach is hereafter applied to the multicast communication link whose receiving-side computer is plurality as an example 4 is explained.

[0059] <Configuration of an example 4> Drawing 14 is the block diagram showing the communication system with which the example 4 of the authentication art by this invention was applied. Here, in the transmitting-side computer 200, a network 400 connects and the server computer (henceforth an authentication processing computer) 100 which functions as an authentication processing computer shows [computers / 300 (300a, 300b, 300c) / three / receiving-side] the whole system

configuration with the multicast communication facility connected by the network 401 here [two or more].

[0060] Since this system is approximated with the example 1 shown in drawing 1 , only difference with the system of drawing 1 is described about each part. As mentioned above, three receiving-side computers 300a, 300b, and 300c exist here, and the network 401 connects with the authentication processing computer 100 respectively. Each receiving-side computers 300a, 300b, and 300c are the same configurations. It replaces with the authentication communication service processing section 111 of drawing 1 , and the application server program 110 of the authentication processing computer 100 is equipped with multicast authentication communication service processing section 111a with multicast communication facility. Here, multicast communication facility means the function to transmit the commo data which the application program 210 on the transmitting-side computer 200 transmitted to the authentication processing computer 100 by three receiving-side computers 300a and 300b and addressing to 300c to these three receiving-side computers 300a, 300b, and 300c. In addition, in drawing 14 , the same sign as drawing 1 shows the same or a considerable part.

[0061] <Actuation of an example 4> Next, actuation of the above-mentioned example 4 is explained. Processing of the application program 210 concerned at the time of an application program 210 transmitting correspondence to the authentication processing computer 100 (application server program 110) in the transmitting-side computer 200 is the same as that of the case (drawing 2) of an example 1.

[0062] In the correspondence which an application program 210 transmits, three addressees are described as recipient information. That is, a format of commo data here comes to be shown in drawing 15 . A transmitting person is expressed by A, the addressee is expressed by B, C, and D, and A-D contains each address information. Correspondence consists of the transmitting person information A and recipient information B, C, and D, and a correspondence body, and commo data consists of this correspondence and a digital signature of the message digest of correspondence so that it may illustrate. By the example 4, receiving-side computer 300b and recipient information D are set [the transmitting person information A / the transmitting-side computer 200 and recipient information B] to receiving-side computer 300c by receiving-side computer 300a and recipient information C.

[0063] Actuation of the authentication processing computer 100 (application server program 110) which received the commo data from the transmitting-side computer 200 is as being shown in drawing 16 . That is, the application server program 110

receives the commo data with which it comes to double the correspondence and the digital signature from the transmitting-side computer 200 first (step S161).

[0064] Next, the application server program 110 verifies the digital signature of the transmitting-side computer 200 by the digital signature verification processing section 113 (step S162). The following procedures perform verification of this digital signature. Introduction and the application server program 110 use the public key of the transmitting-side computer 200 registered into the user public key database 120, and take out a message digest from the digital signature of the transmitting-side computer 200. Next, the message digest processing section 112 newly generates the message digest of the above-mentioned correspondence. And the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest, and if those coincidence is checked, verification of a digital signature will terminate normally. If inharmonious, an error will be notified to the transmitting-side computer 200.

[0065] After verification of a digital signature, the application server program 110 starts the digital signature generation processing section 114, uses the private key of the self-program managed at the private key Management Department 130, and newly generates the digital signature of the message digest of the above-mentioned correspondence (step S163). Then, the application server program 110 transmits the commo data with which it comes to double the above-mentioned correspondence and the newly generated digital signature to the receiving-side computer 300 (step S164).

[0066] As for transmission (step S164) to the receiving-side computer 300 of commo data, the receiving-side computers 300a, 300b, and 300c are repeatedly performed only for the number of the receiving-side computers 300 here 3 times, and a multicast communication link is realized (step S165). Each recipient information can be known by referring to the above-mentioned correspondence. Processing of the application program 310 concerned at the time of an application program 310 receiving correspondence in each receiving-side computer 300 is the same as that of the case (drawing 5) of an example 1.

[0067] <Effectiveness of an example 4> Also in (1) multicast communication link, since the authentication processing computer 100 by which it operates independently by not a public key certificate authority but the single layered structure of a large number systematized by the layered structure as for which each operates in cooperation manages the public key of the transmitting-side computer 200 like the conventional technique, the system which it is flexible and is easy to manage on the aspect of practical use of the public key of the transmitting-side computer 200 can be

built.

[0068] (2) When partner authentication was conventionally performed among two or more addressees using a digital signature, each receiving-side computer needed to receive the public key of a transmitting-side computer for every transmitting-side computer. By the example 4, since the above-mentioned authentication processing computer 100 manages a user's (transmitting-side computer 200) public key collectively, the complicatedness to which each receiving-side computer 300 (300a, 300b, 300c) receives the public key of the transmitting-side computer 200 separately can be excluded, and network traffic, especially the network traffic covering between the transmission-and-reception side computers 200,300 can be decreased. Such effectiveness in an example 4 becomes the part whose number of receiving-side computers increases, and a more remarkable thing as compared with the effectiveness in the authentication communication link between the 2 persons in an example 1.

[0069] The authentication processing computer 100 is equipped with the user public key database 120 in the above-mentioned examples 1 and 4. Moreover, the computer 100 is equipped with the object public key database 160 in the example 2. Furthermore, the agent coordination device 170 is equipped with the agent public key database 174 in the example 3. It is also possible to make this the configuration in which a public key certificate authority manages each above-mentioned public key database as the specification of ITU-X.509 grade. The case where except the user public key database 120 from the authentication processing computer 100, replace with it, and the public key certificate authority of the exterior by the specification of ITU-X.509 grade is hereafter used in an example 1 (drawing 1) as an example 5 is explained.

[0070] <Configuration of an example 5> Drawing 17 is the block diagram showing the communication system with which the example 5 of the authentication art by this invention was applied. Here, the whole system configuration to which the server computer (henceforth an authentication processing computer) 100 which functions as an authentication processing computer was connected to by the network 400 in the transmitting-side computer 200, and was respectively connected by the network 401 in the receiving-side computer 300 is shown. By this example 5, the authentication processing computer 100 is connected with the external public key certificate authority 700 by the network 404 so that it may illustrate. And with reference to the time of verifying a user's (transmitting-side computer 200) digital signature, as a user public key database used, it has in the above-mentioned public key certificate authority 700, and is made as [use / as the specification of ITU-X.509 grade / the

user public key database 710 managed by the public key certificate authority 700]. A user's public key is registered into the above-mentioned user public key database 710. The above-mentioned user public key database 710 is under management of the application server program 110 at the time of verification of a digital signature. Since others are the same as that of an example 1 (drawing 1), in drawing 14 , they give the same sign to the same part as drawing 1 , and omit the explanation.

[0071] <Actuation of an example 5> Next, actuation of the above-mentioned example 5 is explained. Processing of the application program 210 concerned at the time of an application program 210 transmitting correspondence to the authentication processing computer 100 (application server program 110) in the transmitting-side computer 200 is the same as that of the case (drawing 2) of an example 1. A format of the commo data which an application program 210 transmits is the same as that of the case (drawing 3) of an example 1.

[0072] Actuation of the authentication processing computer 100 (application server program 110) which received the commo data from the transmitting-side computer 200 is as being shown in drawing 18 . That is, the application server program 110 receives the commo data with which it comes to double the correspondence and the digital signature from the transmitting-side computer 200 first (step S181).

[0073] Next, the application server program 110 verifies the digital signature of the transmitting-side computer 200 by the digital signature verification processing section 113, after acquiring a user's (transmitting-side computer 200) public key from the user public key database 710 of the public key certificate authority 700 (step S182) (step S183). The following procedures perform verification of this digital signature. Introduction and the application server program 110 use the public key of the transmitting-side computer 200 acquired at step 182, and take out a message digest from the digital signature of the transmitting-side computer 200. Next, the message digest processing section 112 newly generates the message digest of the above-mentioned correspondence. And the message digest taken out from the above-mentioned digital signature is compared with the newly generated message digest, and if those coincidence is checked, verification of a digital signature will terminate normally. If inharmonious, an error will be notified to the transmitting-side computer 200.

[0074] After verification of a digital signature, the application server program 110 starts the digital signature generation processing section 114, uses the private key of the self-program managed at the private key Management Department 130, and newly generates the digital signature of the message digest of the above-mentioned

correspondence (step S184). Then, the application server program 110 transmits the commo data with which it comes to double the above-mentioned correspondence and the newly generated digital signature to the receiving-side computer 300 (step S185). Recipient information can be known by referring to the above-mentioned correspondence. Processing of the application program 310 concerned at the time of an application program 310 receiving correspondence in the receiving-side computer 300 is the same as that of the case (drawing 5) of an example 1.

[0075] <Effectiveness of an example 5> Since each manages the public key of the transmitting-side computer 200 like (1) conventional technique under management of the authentication processing computer 100 which operates independently by not a public key certificate authority but the single layered structure of a large number systematized by the layered structure which operates in cooperation, the system which it is flexible and is easy to manage on the aspect of practical use of the public key of the transmitting-side computer 200 can be built.

[0076] (2) In the partner authentication between the 2 persons who used the digital signature, the receiving-side computer needed to receive the public key of a transmitting-side computer for every transmitting-side computer conventionally. By the example 5, since the above-mentioned authentication processing computer 100 manages a user's (transmitting-side computer 200) public key collectively under the management, the complicatedness to which the receiving-side computer 300 receives the public key of the transmitting-side computer 200 separately can be excluded, and network traffic, especially the network traffic covering between the transmission-and-reception side computers 200,300 can be decreased.

[0077] In addition, by examples 1-5 (drawing 1 , 6, 10, 14, 17), although the transmitting-side computer 200 and the receiving-side computer 300 all show the case of 1 to 1 (it is 1 to 1 set when it is the multicast communication link of an example 4), two or more sets of combination of the transmitting-side computer 200 and the receiving-side computer 300 exists on both sides of the authentication processing computer 100 in fact. Each of each examples [two or more sets of] operates similarly in each class, when it exists such, and the same effectiveness is acquired. Moreover, in examples 1-5, "management" means registration of the public key concerned, deletion, updating, retrieval, reference, etc. about the public key in each public key database.